Security Monitoring of Distribution Automation Systems

Dhiaa Elhak Rebbah

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

July 2021

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Dhiaa Elhak Rebbah**
Entitled: **Security Monitoring of Distribution Automation 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. Jun Yan

_____ External Examiner
Dr. Otmane Ait Mohamed

_____ Internal Examiner
Dr. Mohsen Ghafouri

_____ Thesis Supervisor
Dr. Mourad Debbabi

Approved by _____
Dr. Mohammad Mannan, Graduate Program Director

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

Abstract for Masters

Security Monitoring of Distribution Automation Systems

Dhiaa Elhak Rebbah

Distribution automation systems represent the new generation of power distribution systems in response to the growing interest in smart grids along with the integration of information and communication technologies (ICT). Distribution automation systems leverage advanced ICTs to automate system operation for delivering electrical energy to consumers. With the use of ICT comes the need to protect distribution automation systems from cyberattacks that could impact the operation of such systems, mainly power availability.

In this thesis, the main objective is to assess the security aspect of distribution automation systems. As such, we design and implement a security monitoring platform that allows assessing the dynamics of these systems. In this regard, a digital twin testbed is designed and implemented to simulate smart power distribution systems in near real-time. Moreover, a proposed security monitoring platform is designed and implemented on top of the previously mentioned digital twin testbed. The platform can help monitor the impacts of different occurring incidents and allows executing implemented cyberattacks against the modeled power systems. In addition, it employs AI techniques to detect these attacks.

The specific contributions of this thesis are: (i) the design and implementation of a co-simulation testbed for distribution automation systems using open source software packages; (ii) the design and implementation of an AI-based security analytics framework for distribution automation systems; and (iii) the implementation of cyberattacks targeting distribution automation applications. Various machine and deep learning models are implemented to detect the attacks and different performance evaluation metrics are used to compare different models. The obtained results are competitive and they validate the usefulness of the models in detecting attacks. The co-simulation platform is able to simulate power distribution systems in near real-time, along with an emulation of the IEC 60870-5-104 communication protocol. Also, the platform is capable of simulating big distribution test cases, e.g., the IEEE 123-bus and the IEEE 8500-nodes systems.

Acknowledgments

I express my gratitude to all those that have contributed towards my thesis and to those who have supported my progression towards its completion.

I am grateful to my supervisor, Dr. Mourad Debbabi, for the time and commitment invested in my research. His vast experience and insights within the domain of my research has truly expanded my understanding of the field, both from a theoretical and practical perspective.

I extend my gratitude to Dr. Jun Yan, Dr. Mohsen Ghafouri, and Dr. Otmane Ait-Mohamed for being part of the examination committee and for their evaluation.

I would like to acknowledge the fruitful collaboration with Mr. Mark Karanfil, Mr. Christian Salem, Mr. Afshin Ebtia, Mr. Badis Racherache, Ms. Meriem Ferdjouni, and Mr. Abdullah Qasem throughout this research. In addition, I would like to acknowledge the rest of my colleagues for their support and encouragement during my studies, as well as the many professors who have offered their own insights during the regular meetings concerning the research progress on smart grid security. I am thankful to Dr. Andrei Tudor Soeanu for his corrections on the early versions of this thesis. I would like to acknowledge the support received from NSERC, Hydro-Quebec, and Thales for this project.

Finally, I am deeply grateful to my family for their immense support and encouragement throughout my academic studies. My parents, siblings, and my uncle in particular have shown me vast amounts of patience as I progressed through my studies. For this I am truly thankful, and I love you all dearly.

Table of Content

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivations

Distribution automation systems represent the new generation of power distribution systems. With the integration of ICTs, the operation of such systems becomes easier and more reliable. The automation aspect of distribution automation systems mandates the implementation of different applications, which allow to automate the functioning of these systems. Typical applications include: fault localization, isolation, and service restoration (FLISR) where faults are detected automatically using sensors. Feeder reconfiguration is another automation application that optimizes power loss in the system when sensing that the loss is at a critical level. Such applications take advantage of ICTs to enhance power distribution to consumers. The main objective of these advanced distribution systems is to have more control over the distribution grid. This requires a combination of different technologies allowing for system visibility in real-time. Having a real-time overview of these systems enables faster reaction to critical events that could occur during the operation of these systems.

Distribution automation systems are increasingly deployed as part of the larger modernized grid. According to the Smart Grid annual report of 2018 issued by U.S. Department of

Energy (DoE), it is estimated that the use of automatic fault localization allowed the United States to save around $23 million, as a result of avoiding customer damage costs [4]. Moreover, Florida Power and Light utility obtained a better transformer performance by employing smart meters for real time data transmission to the distribution system's operator. This allowed for a prompt reaction to unexpected shifts in electrical energy usage. Based on Canada's Smart Grid report of 2018, 25 power utilities are already integrating smart demand management [5]. For example, in 2018, Nova Scotia Power utility received approval to deploy a smart meter for every customer using a funding of $133 million [5]. It was expected to complete the deployment of smart meters by 2020 [6]. These recent deployments have been carried out to meet smart grids requirements. Smart grid adoption also allows for large scale integration of renewable energy sources, which can contribute to the reduction of greenhouse gas emissions.

Smart grids are required to use ICTs in their operations. These technologies allow for a better control of the different smart grid domains where smart distribution represents one such domains. The adoption of a set of reliable and fast communication technologies allows to react to events in real time. These events could represent faults caused by either a natural incident or human error. Also, they might occur due to cyberattacks targeting these systems. These cyberattacks could be impactful, damaging, and the resumption of normal operations can range from hours to weeks and even months. For example, in 2015, the sophisticated attack against the distribution system of Ukraine left 230,000 customers without electricity [7]. The attack surface was the distribution system, specifically the distribution management system (DMS) via a malware named "BlackEnergy" embedded in a word document [7]. The malware affected the system in such a way that it caused undesirable changes to the electricity distribution infrastructure "by wiping SCADA server" [7]. This server wiping was caused by a "KillDisk" component that is embedded within the

malware. Once it was inside the SCADA system of the Ukrainian power system, "BlackEnergy" started by destroying all the files inside the servers. The "KillDisk" component that was embedded in this malware was able to overwrite documents and files with random data and make the operating system unbootable [8]. The power outage lasted for a period between 3 to 6 hours [7]. Another attack involved the use of a different malware named "Industroyer", which was also used against the Ukrainian power grid on December 2016 [9]. This malware is more sophisticated compared to "BlackEnergy", "StuxNet", and others since it can use several backdoors to enter the system [9]. After entering the system, it launches several ICS communication protocols messages with malicious payloads, e.g., IEC 104, IEC 101, IEC 61850, and OLE for Process Control Data Access [9]. This means that the infected device becomes a rogue device within the network. "Industroyer" also contains a Data Wiper, which allows it to delete all the data inside the system [9]. Since distribution systems are part of the critical infrastructure, they must be able to cope with any type of adverse events. These systems must be resilient to faults and cyberattacks in order to maintain the availability of electrical energy.

1.2 Problem Statement

The purpose of this research is to design and implement a security monitoring platform that will detect cyberattacks against distribution automation systems.

1.3 Objectives

The objectives of this thesis are as follows:

- Design and implement a co-simulation testbed allowing the simulation and emulation respectively of power distribution systems and an industrial communication protocol, such as the IEC 60870-5-104.

- Design and implement automation solutions for the most important distribution automation systems' applications: (1) Fault localization, isolation, and service restoration, (2) voltage regulation, (3) feeder reconfiguration, and (4) bad data detection.
- Craft and execute simulated cyberattacks targeting the aforementioned distributed automation applications.
- Design and implement a security monitoring platform able to detect the simulated cyberattacks by leveraging machine and deep learning techniques to detect false data injection targeting the automation applications.

1.4 Contributions

The main contributions of this thesis are the:

1. Elaboration of a realistic real-time digital twin framework that can simulate distribution automation systems, using mainly open-source resources, including the emulation of the communication protocol IEC 60870-5-104. We implement two power models: the IEEE 33-bus and the IEEE 123-bus systems. The first one is selected as it has heterogeneous loads to see the impacts of different cyberattacks. The second one is selected to test the scalability aspect of our co-simulation platform by choosing a larger system with more components.
2. Elaboration of a security monitoring platform employing machine learning and deep learning techniques to detect cyberattacks targeting the implemented automation applications.

1.5 Thesis Structure

The remainder of the thesis is structured as follows. Chapter 2 provides the needed background on the key concepts underlying distribution automation systems, power distribution systems, communication protocols, and detection algorithms. Chapter 3 provides the state-of-the-art literature review. Chapter 4 details the employed methodology for the implementation of the co-simulation testbed. Chapter 5 discusses the experimental setup used to conduct simulations, exercise scenarios, and the security monitoring platform along with the simulated attacks. In addition, it presents an evaluation of the obtained results to compare the performance among several techniques employed to detect the simulated attacks. Finally, Chapter 6 provides the concluding remarks and the future research directions.

Chapter 2

Background

In this chapter, we discuss the key distribution automation system concepts, the general aspects, and the component parts involved in such system in terms of communication technologies. First, we provide a general explanation and related smart grid definitions along with a discussion on the communication technologies involved in the operations of the smart grid in the context of the existing international standards. Second, we illustrate the distribution automation systems in details, as integral components of the smart grid, along with the related applications. Finally, we discuss the cyber attacks targeting the smart grid in general along with related detection techniques.

2.1 Smart Grid

The smart grid involves the integration of communication technologies to enhance the functionalities of the traditional power grid, which uses the Supervisory Control And Data Acquisition Systems (SCADA). This new generation of power grids facilitate the two-ways communication between the power utility and the consumer. New smart devices are also integrated, that are considered to be smart or "intelligent". These new devices are called Intelligent Electronic Devices (IEDs). The IEDs allow control, protection, data alignment,

data aggregation of measurements among other things that are important in smart grids. Also, IEDs collect analog signals of active and reactive power, current, voltage, frequency, and several other types of measurements needed to define the present state of a system. The IEDs also convert in a real-time manner the raw data and it is ready to be fed to applications monitored by operators overseeing the power system. At the consumer level, smart meters are implemented to have a real-time view of power consumption. These meters generate and transfer measurement data to the power utility. Along with the use of this data for billing purposes, it is used as well to keep the balance between customer load demands and the amounts of generated power that the utility has to provide. All of these intelligent devices are what make the Smart Grid smart.

The different domains of the power grid are to be enhanced by the smart grid. This includes: generation, transmission, and distribution. For generation, the smart grid adds the aspect of smart loads and distributed energy resources. By using different energy resources, the loads generated are combined to satisfy the needed load demands by consumers. These different energy resources can be: combined heat and power resources, energy produced using diesel engines, or even renewable energy resources. The smart grid also benefits from Electric Vehicles (EVs) by using the cars that are in idle mode with a full-charged state as load suppliers in case of a need for additional demanded loads. In terms of distribution, the smart grid introduces a new type of systems, which is the distribution automation system. This type of systems allows more automation during power distribution to consumers in a smart way. The addition of smart meters and faster polling of the measurements allows a near real-time view of the system. This allows a better load demand satisfaction on the available load the system has. The new distribution systems also requires having IEDs allowing fault detection. These IEDs can sense a fault in a line and notify immediately the distribution system's operator to take action. In order to stabilize the system, different applications must be in place. One of these applications is the feeder reconfiguration. This

application can automatically re-configure the topology of the power distribution system on how the loads should be satisfied. This will benefits the system from having less power loss. There are several other applications in place to have an automated monitoring and control over power distribution systems.

Briefly, the smart grid allows power utilities to have a more efficient, reliable, automated power grid. This is achieved by integrating IEDs and different control applications. This integration allows a real-time monitoring of the power grid. It also helps reacting to any changes occurring in the system faster. However, since the adoption of the smart grid was initiated in 2007, power utilities started embracing the new technologies and smart devices (e.g., IEDs) made by various vendors. For marketing reasons, it is not necessary that all vendors design the same types of devices with the same characteristics. Also, the way these IEDs communicate requires specific communication protocols, but which ones? In this case, standardisation is necessary to specify the type of communication technologies and what characteristics could be suitable for the multiple existing vendors. Among the existing standards for smart grids is the IEC 61850 which enlists the different communication protocols, data types, and IEDs characteristics. Fig. 1 shows the design of the smart grid along with its components.

2.1.1 Smart Grid Domains

The smart grid targets the different domains of the traditional grid (e.g., transmission and distribution) and enhance these domains by adding IEDs, new automation and control applications, new communication protocols, new standards, etc.

Transmission

The transmission domain in power grids is the phase were the generated electricity from a power plant gets transmitted as a bulk to an electrical substation. This phase uses a

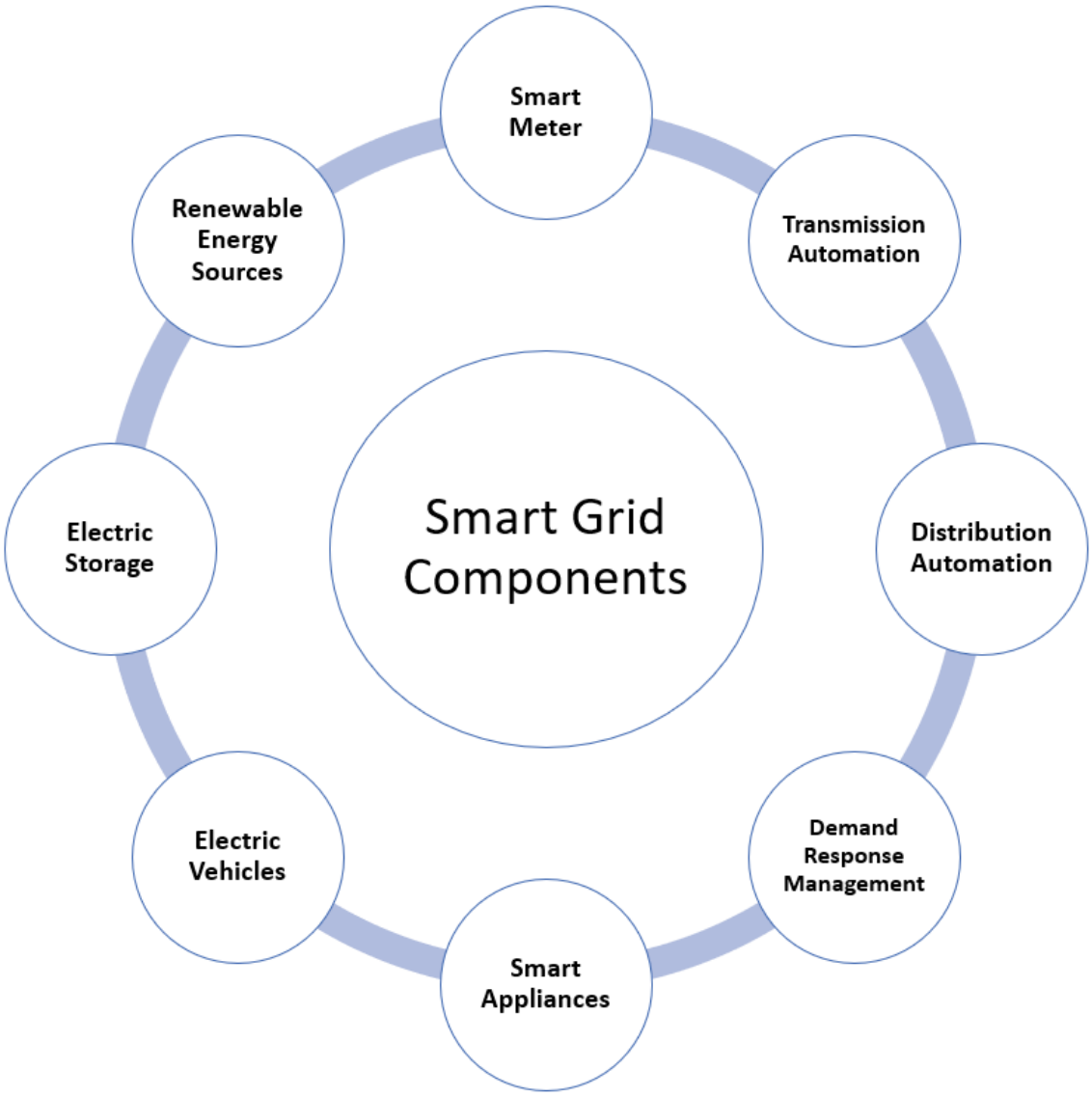


Figure 1: Smart Grid Components [1]

series of interconnected transmission lines called a transmission network. This network requires enhancements stated in the the IEC 61850 standard. These enhancements include the addition of different technologies in the power transmission system.

Among these technologies: the flexible AC transmission system technology (FACTS), the high voltage direct current technology (HVDC), the dynamic thermal rating technology, the addition of synchrophasor technologies, etc. These technologies allows the transmission system to be self-healing, tolerant to attacks by mitigating and being resilient to

physical and cyber attacks, and it becomes able to accommodate wide variety of of supply and demand.

The addition of the mentioned technologies requires adding new communication protocols. The added communication protocols allows a faster and reliable data transmission of the required information and values of the different technologies. These protocols also contribute in a faster reaction to certain situations when the transmission substation is required to take action.

Among the communication protocols we mention the IEEE C37.118 and the IEC 61850-90-5. These protocols are used for Phasor Measurement Units (PMU) and Phasor Data Concentrator (PDC). These protocols allow a faster interconnection between different substations. Since the smart grid primarily focuses on leveraging the synchronized current/voltage amplitudes and phase angles measurements coming from the PDCs to have a real-time overview of the system. Therefore, these communication protocols are in place to achieve such goal.

Distribution

The power distribution system is the last phase between the main grid and the end consumer. It consists of a distribution substation where the high voltage power gets lowered via power transformers to medium and low voltages. The process of lowering the voltage is required as the end consumers are low and medium voltage users depending on the types of loads, e.i, residential, commercial, or industrial. As part of the domains of smart grids, it is required to enhance the power distribution system as well. This happens by adding several technologies, components, and communication protocols.

The power distribution system becomes the distribution automation system. By adding automation applications, such as FLISR, automatic voltage regulation, automatic feeder reconfiguration, and several others. This allows the energy distribution to be more automatic,

reliable, keeping in mind the availability aspect of electricity. These applications use different measurements as input sent directly to the Distribution System's Operator (DSO). This results in taking action by generating specific commands based on the received, in real-time, measurements. The DSO is the main controller in the distribution automation system. Controlled by a team of people overseeing the functioning of the system in real-time. The DSO is required to checked the demanded loads and satisfy it based on the amount of available loads to keep the system in balance.

Also, the DSO is required to check the different automation applications in place to see if any application is needed to, for example, enhance the voltage by launching the voltage regulation, or whether a fault is detected by the FLISR and what isolated line needs to be fixed. Another important required job that needs to be done by the DSO is to check for anomalies in the system, caused by either faults or cyber attacks. The DSO is required to have different anomaly and intrusion detection mechanisms put in place. These mechanisms allow detecting any types of anomalies to react fast to keep the system from failing, protecting the system's component, and keeping power availability at all time.

2.1.2 Smart Grid Standards

The availability of several vendors and communication technologies results in the challenge of interoperability. This challenge is resolved by standardizing the smart grid. Several working groups brought an international standard for the smart grid to existence, knowing that there are different standardization bodies and related committees. These include, the American National Standards Institute (ANSI), the National Institute of Standards and Technology (NIST), the International Electrotechnical Committee (IEC) and several other committees, which proposed different standards; The IEC 61850 that defines communication protocols used for IEDs at electrical substations. It specifies mapping to standard communication technologies which are; Manufacturing Message Specification (MMS), Generic

Object Oriented Substation Event (GOOSE), and Sampled Analog Values (SMV).

The IEC 60870 standard defines the communication network for different applications, such as the communication protocol suitable for microgrid projects and the implementation of distributed grid generation. Then, ANSI C12.18, C12.19, and C12.22, specified the implementation of Advanced Metering Infrastructures (AMI), provided specifications for data exchange between devices, and specified the communication protocols to be used for data exchange.

2.1.3 Smart Grid Communication Protocols

The smart grid focuses on adding faster and reliable communication protocols. There are several existing technologies that can be used to satisfy the time requirements of inter-arrival time for the data from a node to another, based on specific applications (e.g., collecting and transmitting measurement data at a higher rate). Therefore, we need to use more reliable communication technologies. In the early phases of smart grid adoption, several power system operators and research institutes mainly suggested the use of existing communication protocols and technologies (e.g., Internet, LAN networks, WIFI, ZigBee and Mesh networks).

Several power utilities started embracing new types of technologies, such as Power Line Communication, which allows using the existing transmission lines for data transfer. Another method is to use phone lines or what is known as Digital Subscriber Lines (DSL). The different communication methods have the same end goal: having each node in the power system communicate with the control center in order to have a clear view in real-time of the system state in general [10]. There are several advantages and disadvantages of each technique. However, the key relevant aspects are the speed of data transfer and the range of transmission of each technology, as detailed in Table 1.

Table 1: Communication technologies used in the Smart Grid

Technology	Spectrum	Data Rate	Coverage Range	Applications	Limitations
GSM	900-1800 MHz	Up to 14.4 Kbps	1-10 Km	AMI, Demand Response, HAN	Low data rates
GPRS	900-1800 MHz	Up to 170 Kbps	1-10 Km	AMI, Demand Response, HAN	Low data rates
3G	1.92-1.98GHz 2.11-2.17 GHz (licensed)	384 Kbps-2MBps	1-10 Km	AMI, Demand Response, HAN	Costly fees
WiMAX	2.5 GHz, 3.5 GHz, 5.8 GHz	Up to 75 Mbps	10-50 Km (LOS) 1-4 Km (NLOS)	AMI, Demand Response	Not widespread
PLC	1-30 MHz	2-3 Mbps	1-3 Km	AMI, Fraud Detection	Noisy channel environment
ZigBee	2.4 GHz 868-915 MHz	250 Kbps	30-50 m	AMI, HAN	Low data rate, short rage

IEC 61850

As mentioned in Section 2.1.2, the IEC 61850 standard defines the communication technologies used for data exchange between IEDs in substations. In this thesis, we focus more on the communication protocols used in a smart grid environment. Thus, we first provide a background for this standard. The IEC 61850 standard consists of ten parts. Each part defines a specific area or application. However, the main goal of this standard is to achieve the substation automation by adding communication technologies along with the data exchange happening between IEDs installed within the substation. The standard specifies protocols, data, and devices characteristics. In the standard, the specifications for communication protocols are mentioned from part 6 to part 9 starting from the data exchange for substation and feeder automation, to specific new communication protocols. Such protocols include Generic Oriented Object Substation Event (GOOSE), Sampled Analog Values (SV), and Manufacturing Messages Specific (MMS) protocols. Definitions for each protocol will also be provided in this section.

The standard also defines the architecture of the smart grid substation, as shown in Fig. 2. Based on the architecture, and the applications involved in the substation automation, a fast data exchange rate is often required, with a fast time to live for the transmitted data. For example, GOOSE has a limited allowed Time-To-Live (TTL) for the messages, which

means that it requires a very fast communication technology using the communication protocols specified in the standard. Several other specifications are provided in the IEC 61850. To achieve security and reliability of the substation automation, the standard specification must be respected. We must mention that the standard does not provide details about security for data exchange to ensure confidentiality and data integrity. There are different standards considered as security standards for the IEC 61850 (e.g., part five of the IEC 62351, which specifies the security procedures to secure the communication protocols for substation automation and different applications for the smart grid).

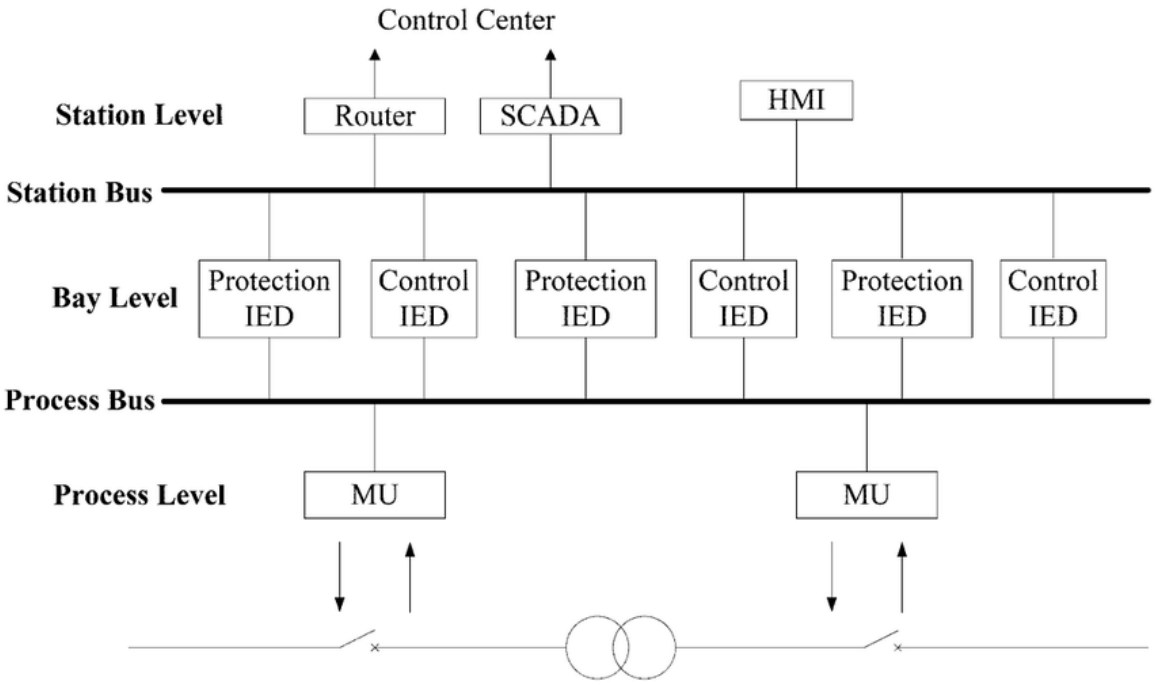


Figure 2: Substation Architecture

Generic Oriented Object Substation Event

As mentioned in Section 2.1.3, the IEC 61850 specifies the data exchange protocol between the bus and the substation level to get the status of circuit breakers and relays and send commands to these intelligent electronic devices in the grid. Part 7 of the IEC 61850 and

specifically part 2 specifies the way the data exchange is mapped in the Generic Oriented Object Substation Event (GOOSE) communication protocol.

Among the main applications that GOOSE is used for is sending tripping commands from relays to circuit breakers and receiving status from IEDs deployed in the substation. These IEDs could involve a circuit breaker communicating to a relay, or vice-versa. This type of communication requires a fast data transmission rate, which is delivered by GOOSE in a four milliseconds duration per message. GOOSE can be used for several other applications, but in the standard it mainly covers the status of IEDs and the commands that should be sent via this protocol.

Sampled Analog Values

Sampled Analog Values (SV) as the name implies, represents a communication protocol used for data exchange between Merging Units (MUs) and IEDs in digital substations over Ethernet. It is specified in the IEC 61850 standard. This protocol has a sampling rate of 4800 messages per second. SV is mainly used to provide the substation control room with the actual real-time active power, reactive power, current, voltages, magnitudes, frequencies, and several other types of measurements collected from MUs.

These IEDs can be directly deployed in any type of substation whether it is a generation substation, transmission, or a distribution substation. Due to the fast sampling rate previously mentioned, SV satisfies the needs of collecting measurements in real-time, which is required for certain applications of substation's automation.

Manufacturing Messages Specific

This communication protocol is described in part 8 of the IEC 61850 standard, which specifies a communication protocol that enables data exchange in real-time between processes of different devices in the field, in this case IEDs in the substation. Manufacturing Messages

Specific (MMS) helps re-configuring new IEDs while being deployed in any substation. Also, it helps with the interoperability aspect while having several IEDs from different manufacturers. This is achieved by adding the new devices to the Substation Configuration Language (SCL) file, which is the core configuration file of any substation. This file contains all the IEDs deployed and installed, along with the communication topology of the substation itself.

Basically, MMS helps to add new lines to this file based on a protocol agreement mentioned in IEC 61850 standard. In order to configure the SCL file we are required to use MMS, since it is the only communication protocol suitable for the substation to add new IEDs.

IEC 60870-5-104

We provide next a brief background of the IEC 60870-5-104 (IEC 104) communication protocol, which is used for several applications. The IEC 104 is the European version of DNP3 that is used in North America for microgrids and power distribution systems. It is a communication protocol on top of the TCP protocol that follows a Master/Slave scheme. However, in the context of TCP, it adheres to a client/server scheme, where the Master is the Server and the Slaves are the TCP Clients.

Slaves can be the different communicating nodes in power distribution systems. These nodes differs based on the application IEC 104 is used for. For example, for measurements reporting, the Data Aggregation Units (DAU) that are responsible to collect different power measurements for a neighborhood to the DSO. In this case, the IEC 104 slaves are the DAUs in the power distribution system, and the IEC 104 Master is the DSO. In IEC 104, the allowed Time-To-Live (TTL) for messages is between 10 to 15 seconds. After 15 seconds, the communicating nodes declare a time-out for packets resulting the denial of that packet. In terms of security, IEC 62351-7 mentions several specifications on how to

secure the IEC 104 protocol by using TLS and encryption schemes to secure the end-to-end communication at the transport layer.

As such, Man-in-the-middle type of attacks will not be viable.The IEC 104 protocol is effective for distribution automation systems due to its rapid data transmission rate up to 4 messages/second. This provides enough room for huge amounts of data to arrive to their destination in time with the sufficient TTL explained before. It is safe to mention that the IEC 104 can be modified to suite the different applications of DA since it supports different types of data.

2.2 Power Distribution Systems

The use of power distribution systems represents one of the cornerstones of the thesis. Thus, we conducted a review of the relevant documentation, in order to get a proper definition of the PDS, as it is part of the power delivery infrastructure that transforms to medium voltage levels the power coming from the transmission substation at high voltage [11]. The medium voltage levels in distribution systems range from 600 V to 35 kV. However, with the use of transformers, voltage values are reduces from high voltage (230 kV) to low voltage (120/240 V) for consumers use. There are two types of electrical distribution systems; radial or network [12]. The radial is a system that is arranged like a tree where each consumer has one source of supply, where the network type of systems has multiple sources of power supply functioning in parallel. The radial is commonly used in the US, where it has one main power source, which is the transmission grid [12], going to the consumer loads.

2.3 Distribution Automation Systems

In this section, we provide the necessary background, as well as an elaborate definition of Distribution Automation Systems (distribution automation system). Such systems are considered as a more evolved type of Power Distribution Systems (PDS). Briefly, the PDS is the last phase of power delivery to the consumer. It is the checkpoint between the transmission substation and the distribution substation. The PDS contains voltage transformers, that are responsible for transforming high voltage from the transmission lines to medium and low voltage, depending on the use case: If the power is meant for industrial or commercial consumers, it would be medium to low voltages; in the case of residential consumers (e.g., neighborhood or individual housing units), it would be medium voltage for a neighborhood and low voltage for household appliances.

The PDS system also contains several other parts, not just transformers. It includes tap changers, reclosers, capacitor banks, relays, and different other components, which are required for the functionality of such system. However, there is less automation in the PDS. This means that it is not that ”intelligent” if we are considering the transition to the smart grid. Thus, there is a need to improve this system, which is where distribution automation systems are aimed at. A power distribution system is responsible for distributing power to consumers, meaning that other applications such as metering are part of the power distribution system as well. For billing purposes, there are meters deployed at each housing unit. These meters send data, on a daily basis, with a sampling rate of 30 to 45 minutes for each unit. This means we do not have a real-time view of the power consumption at each household. This and several other limitations of PDS need to be addressed in the next version of the PDS.

Therefore, the distribution automation system represents the new version of PDS that, in addition to several other new benefits, is also addressing the limitations mentioned before. Distribution automation systems are focusing on more automation compared to the

PDS, by having faster communication protocols, more intelligent electronic devices, and several other applications for automation and control. By taking into consideration the fact that power quality is important during power distribution phase, distribution automation systems consist of the the same components of the PDS. However, there are additional new applications (e.g., Volt/Var Control, Automatic Feeder Reconfiguration, and several other applications), for which we will provide definitions and explanations in this section. Thanks to the applications implemented for distribution automation systems, recovery from faults is accomplished more quickly. For example, using FLISR allows localizing faults in near real-time, thanks to the sensors deployed in the distribution substation at each feeder.

By knowing where the fault is, we can easily isolate the affected area. Then, by using another type of applications, namely Feeder Reconfiguration, we can easily reconnect the affected area using tie switches to provide power until the affected feeder is fixed. The recovery from outages is performed faster compared to conventional ways (e.g., waiting for phone reports from consumers to get alerted that a fault exists).

The emergence of smart grid technologies, along with the rapid growth of communication technologies, mainly the Internet of things, implies the urgency of enhancing existing power distribution systems. This involves integrating specific communication systems for an automated distribution grid and leveraging the data gathered from all the nodes in a grid network. It is important as well to mention that a communication infrastructure already exist in traditional PDS. This is the SCADA system, which uses remote terminal units that are transmitting a significant amount of data but with minimal automation [13]. The automation aspect is added by implementing applications and adding them to the system itself. These applications are explained thoroughly in [14]. Some of these applications are: Automatic customer billing, where we take advantage of advanced metering infrastructures and calculate the amount of power usage on a monthly, daily, or even hourly basis.

Among the mentioned applications in [14], we have implemented in our system the following: (i) state estimation which involves gathering measurement data in order estimate the state of a system, using different techniques (e.g., weighted least square (WLS) [15] and machine learning techniques [16]) to understand whether the system is in normal conditions; (ii) Volt/VAR regulation, by using the measurements of the voltages coming from the end nodes of a system − this allows to detect under or over voltages, and to automatically let the tap changer of the transformer regulate the values of the tap number to lower or increase the voltage in the whole system [17, 18]; (iii) feeder reconfiguration, where the goal is to minimize the energy loss in the system [19] due to the losses in transmission lines, using automatic switching and re-closing mechanisms − this involves changing the topology of the network to a better one, taking into account the best topology that allows having minimal power loss.

The last application we have implemented is (iv) FLISR. This application consist of using sensors that locate the fault(s), isolate the faulty area, and then enable strategic switches (closing/opening of reclosers) to restore the system until clearing the fault(s) [20]. Among the different available applications to have in a distribution automation system, we have: Load modeling and forecasting [16], and Remote connect/disconnect [21].

2.4 Distribution Automation Systems Applications

Among the key aspects that helped to transform the previously existing power distribution systems into the distribution automation system, are the applications that help the automation. Most of these applications take a role in adding more automatic features in terms of detecting faults, controlling the voltages, re-configuring the feeders.

Several other applications are executed automatically, and most importantly remotely. Thanks to the integration of communication technologies, it becomes easier to control, monitor, and maintain the PDS stabilized. We provide, in this subsection, definitions of

the most important applications in the distribution automation systems. We also provide an explanation for each application and its role in the system, since we have implemented each mentioned application.

2.4.1 Volt/Var Regulation

As previously mentioned, power quality is the most important thing in the power distribution system. This means that the voltage levels at each node of the system should be firmly withing the allowed thresholds, especially at the end nodes. If the nodes at the end of the feeders present an under-voltage at peak hours, when all the customers are typically using higher levels of power, the end nodes would get an unscheduled under-voltage. To fix such an issue, there is an application named Voltage Regulation, or Volt/Var Reconfiguration. This application considers the voltages at the end nodes as an input. If the voltage values go below the per unit (p.u.) values, the output of the application is a command to the Tap Changer that is implemented at the transformer level of the system. This makes the system increase the voltages in the system until the point of reaching the appropriate p.u. values of the system. In case of an over-voltage, the command to the tap changer is to decrease the voltage values, until getting below the appropriate p.u. values.

2.4.2 Fault Localization, Isolation, and Service Restoration

FLISR is an application that takes benefit of the technology of sensors. In the enhanced grid, sensors are deployed at every electric pole. This means that every electric line we see, has a sensor from both ends. Among the different uses of this technology is the sensing of under or over-voltages, under or over-currents, and outages, along with several other data that can be gathered from sensors. As long as we can detect outages, we take benefit of such information using the FLISR application. After detecting the localization of the fault, the application isolates the area affected by this fault by running a calculation to

know which loads to deactivate from the feeders. Also, it calculates which loads should remain functional, and closing (activating) the tie switches used in case of a fault. These switches are opened in the basic settings of any power distribution system since the power distribution system is in the radial state. This means that the system only functions in a one-way flow of data without the existence of loops. The tie switches are put on the end of each feeder so that while isolating faults, in case of a fault in one feeder, the tie switch would be closed to get power from the neighbor feeder. Thus, the loads will be satisfied without causing any issues until the fault is cleared. This is considered as the service restoration phase of the application. The use of sensors technology, and the automatic execution of all procedures underlie the key benefits of FLISR: quick response times to faults (by rapidly detecting them), isolating the affected areas before more damage could happen, and quickly restoring the service (without taking hours to fix outages).

2.4.3 Feeder Reconfiguration

This application aims at enhancing power quality in the system, by checking the losses of the system and suggesting a new topology of the system that could reduce power losses. In every PDS there is an amount of power that is considered as loss, which power system operators aim to minimize, by changing the topology of the system. However, the feeder reconfiguration application is triggered once in a while, considering that power loss is happening in a regular way, only if the operator determines that power loss is exceeding established thresholds already set in the system.

The inputs of this application, as previously mentioned, are the power loss values along with the current topology of the system, which can be gathered by checking the status of the switches at each load present in the system. The output of the application is the set of load switches to deactivate and the set of tie switches to activate. This way, the whole topology of the system changes while maintaining the system functional along with a power loss

reduction in the system. This is one of the applications that we have implemented in our distribution automation system along with the previously mentioned two applications, as they are of key importance.

2.4.4 Other Applications for Distribution Automation

There are several other applications for distribution automation systems (e.g., energy theft detection, electric vehicles integration, equipment monitoring). These applications can be implemented in distribution automation systems. However, it depends on several consumer specific criteria. It depends on whether the consumer(s) have electric vehicles or whether a house is smart by using smart plugs, and smart monitoring devices. It also depends on specific communication protocols, and accepting to send to the utility real-time data with the power usage of each device. Since power utilities cannot force a client to have these specific devices, these applications are used, implemented, but not heavily targeted by cyber attackers compared to the three applications previously mentioned.

2.5 Cyber Security Threats in the distribution automation system

Like every system that uses communication technologies and protocols, distribution automation systems are prone to cybersecurity threats. These cyber threats typically involve compromising intelligent electronic device, attacks over the network, infiltrating the network, etc. The main goal of an attacker pursuing any of these threats is to harm the grid in any way (e.g., cause financial losses to power utilities, damaging power utility devices, which are very costly, or even leveraging the private information of consumers for nefarious purposes).

Therefore, it is important to have the smart grid secured as much as possible, by securing the communication infrastructure and maintaining real-time monitoring of the system. In this section, we provide background information about the possible cyber threats against smart grids in general, and against distribution automation systems specifically.

2.5.1 Network Scanning Attacks

Network scanning attack allows an attacker to know the entry points to a network. The first step to infiltrate a network is to know from where to enter. The scanning attack allows an attacker to know the opened port numbers in a network. This information can be critical for any type of networks supposing that the attacker already gathered information about a port number left open. For example, if, for any reason, port 21 or 22 were left open which are port numbers used by the File Transfer Protocol, this will allow an attacker to embed a malware that can be used as a backdoor. This backdoor could be used to grant a full access into the network.

2.5.2 Sniffing Attacks

Sniffing attacks comes after getting access into the network. A packet sniffer is a tool that allows the attacker to see the communicated nodes. Since the packet header is not encrypted, the packer sniffers allows the attacker to see the source and destination of any packet. Packet sniffing is helpful to an attacker to have a general idea about the topology of any network. The packet header contain critical information, such as, source and destination IP, source and destination port numbers, length of the packet, the protocol, current timestamp, etc. An attacker can guess through these information the intention of that packet, e.g., a measurement or a tripping command.

2.5.3 Man-In-The-Middle Attacks

Once gaining access into the network, an attacker can act as a Man-In-The-Middle (MITM) attacker. Such attack can happen in secured and unsecured networks. An attacker can be granted access through the network by, for example, stealing credentials, installing a rogue device into the network, taking control over a connected device within the network, or via a supply chain attack by changing settings of a device intended to be installed in the network.

A MITM can drop, delay, modify, replay, or forge packets, depending on the security of the network. In the existence of data integrity mechanisms, a MITM can only drop or delay packets. In the lack of such mechanisms, a MITM can intercept and modify packets. The attacker can also forge a packet and sends it to any intended destination.

2.5.4 Packet Dropping Attacks

In the smart grid communication network, the availability of information is an important thing, to an extent that some applications require the availability of some information to function properly. This information could be a confirmation of a request between nodes, the state of a device to send the next command based on that state, or other required information. For example, GOOSE requires the status of a circuit breaker to be sent to the relay, in order to know if a tripping command is a viable option or not. In such case, a MITM attack can be executed, assuming that an attacker knows when an intercepted packet containing that tripping command is sent from the relay to the circuit breaker. Thus, the attacker could drop the packet easily and avoid the tripping command from reaching the goal node, which is eventually the circuit breaker.

As a countermeasure, among the requirements of GOOSE, there should be a confirmation of the tripping command. This confirmation is sent from the circuit breaker back to the relay. If the relay does not receive the confirmation packet, it should keep re-sending the tripping command until receiving the confirmation. However, if the attacker is smart

enough to hold the confirmation packet as well, there is a threshold of time to try until reaching the time-out.

2.5.5 Packet Modification Attacks

Packet modification implies that the attacker is already within the network acting as MITM. Packets can be seen in clear text if there is a lack of data integrity mechanism or encryption. In the existence of such mechanisms, an attacker can take control over a device in the field. This should grant the attacker access to the encryption keys.

Once the packets are seen in plain text, an attacker could falsify correct information by modifying the packet's content. The attacker could change the packet raw data no matter what the content of the packet is. For example, if the packet contains a tripping command, the attacker could change the tripping value to avoid the tripping action from happening. Also, the attacker can change measurements within packets.

2.5.6 Denial of Service Attacks

The operation of the new digital grid relies on the full time availability. A Denial of Service (DoS) attack is the intention of the attacker to render the system or a device within the system unavailable. The attacker disrupts the targeted device by flooding it with requests to keep actual legitimate packets from communicating with this device.

2.5.7 False Data Injection

False data injection attacks aim to mislead the control centers to taking false actions based on false received information by tampering with the data. This type of attacks implies that the attacker compromises sensor readings in a tricky way that undetected errors are introduced into calculations of state variables and values [22].

Chapter 3

Literature Review

In this chapter, the state-of-the-art addressing the simulation of distribution automation systems is reviewed. Alongside, we review and compare existing power simulators and network emulators. This chapter also includes a general overview on various cybersecurity threats targeting distribution automation systems and their automation applications. We also review the existing security monitoring techniques leveraging machine learning and deep learning algorithms. Thus, this chapter summarizes the most important works related to distribution automation systems, highlights the importance of such systems and the limitation of each reviewed work, and identifies key research gaps.

3.1 Simulating Distribution Automation Systems

In this section, we discuss the relevant works tackling the simulation of power systems and the communications aspects, as well as the tools used in this context. First, we review several works discussing the use of MATPOWER from MATLAB, which is the most used tool in power simulations. McDermott *et al.* [23] use MATPOWER as a tool to model the schemes of the distribution automation using a control system overlay. The authors also use a tool called OpenDSS, implemented by the Electric Power Research Institute (EPRI).

Using this tool, the authors implement a simulation interface to the software modules of the distribution automation, along with the control system that issues various commands that can be sent externally from outside resources. These include sending 'Open' and 'Close' commands for switches. McDermott *et al.* [23] also implement, thanks to the built in functions in MATPOWER, different applications for the control logic of the distribution automation. However, the authors did not include any ideas about the implementation of typical applications used in the distribution automation, such as, voltage control [23]. As for the communication infrastructure, the authors did not include any details.

In contrast, several works published more recently, such as Garau *et al.* [24], use a different software for power simulation, namely DIgSILENT from Power Factory, along with OMNET++ and/or OPNET. It is well known that OMNET++ and OPNET are both communication simulators, both of which allow combining power and communication in order to have a co-simulation platform. Another method to simulate distribution automation systems is the combination between Python and MATPOWER for the implementation of the control logic. Among the notable contributions using this method, the work of Garau *et al.* [24], provides a comprehensive implementation of the FLISR application in distribution automation systems. As for the communication protocol used, the authors do not consider using a standard communication protocols for these systems. Even though OMNET++ only simulates a network with a specific number of nodes, using the COM interface linked in DIgSILENT (implemented in C++), is sufficient to collect all measurements data. Then, the data is sent via a communication technology available in OMNET++, such as, LTE, GSM, GPRS, EDGE, UMTS, etc. While the aforementioned work employs UDP as communication protocol, this is not a standardized communication protocol such as DNP3, MODBUS, or IEC 104.

Elkadeem *et al.* [25] provide a distribution automation system simulation framework.

Although the authors provide less information about the tools used, among the contributions of this work is a distribution automation system simulation working with various implemented applications. The most important applications that are implemented in this paper are: FLISR, Voltage/Var control, Distributed Generation Resources Management application (DGRM), Optimal Feeder Reconfiguration (OFR), Automatic Meter Reading (AMR). Also, the communication gateway is considered as a network simulator that simulates IEC 60870-5-101 protocol and the data is not generated but gathered from the SCADA of a power utility.

Bian *et al.* [26] provide a co-simulation testbed for smart grids using OPAL-RT and OPNET. The intention of this work is to analyze the performance of different smart grid domains, including the distribution automation systems. The setup used in this study is more realistic since it employs an emulation of the network. The authors show how the power aspect of smart grids is simulated using OPAL-RT digital run-time simulator. As for the data exchange protocol, the authors indicate that UDP is used.

Guan *et al.* [27] propose a simulation testbed for feeder automation in distribution automation systems. The software, named DATS-1000, uses a simulation of the IEC 60870-5-104 communication protocol. Also, the tool allows simulating power distribution systems along with simultaneously simulating the network. Thus, it is considered to be a network simulator rather than a power systems simulator [27]. However, the idea is to collect data from a real-time database containing power measurements. The collected data is transmitted over IEC 104 simulated communication network. Moreover, the authors show the detection of faults and how the feeder automatically re-configures itself to remain resilient during faults [27].

The works reviewed in this chapter are among the most cited ones. Nevertheless, we notice a lack of existing works tackling the use of OpenDSS-G for the distribution automation

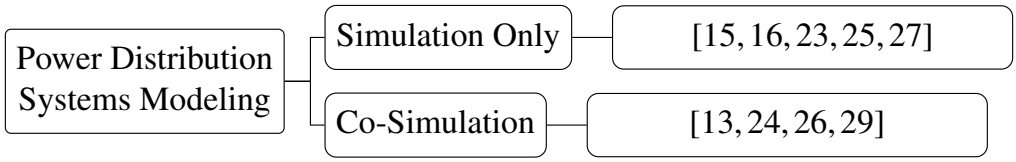


Figure 3: Taxonomy of Power Distribution System's Co-Simulation.

system simulation. However, Montenegro *et al.* [28], detail the main tool used by the creators of OpenDSS. The authors explain the way OpenDSS can be used to simulate power distribution systems, by using the COM interface available in the tool. The authors also provide a way to simulate various communication aspects of the distribution automation system using OMNET++ along with an implementation of various automation applications in C code. The only problem with OpenDSS, is the difficulty of using the tool, as it is a command-line based tool, in contrast to their newly released tool, namely OpenDSS-G.

Based on the type of simulation used in the reviewed works, Figure 3 shows a general taxonomy of the prominent research works dealing with the modeling of distribution automation systems.

3.2 Cybersecurity Threats Targeting Distribution Automation Systems

In this section, we review several works in the literature that are addressing the cybersecurity of the distribution automation system, either in general, or in relation to specific applications implemented in the distribution automation system.

Among the more recent and often cited ones, 15 different works discussing the security of either the distribution automation system specifically, the smart grid in general, or a specific distribution automation system application are selected [30–44].

The smart grid is considered as a part of critical infrastructure. The 'smart' aspect resides in the addition of communication technologies, the adoption of computer algorithms

to control the whole power grid, and the reduction of human involvement. Nevertheless, this is not an all encompassing solution. There are of course obvious benefits in terms of operational reliability and efficiency. The integration of smart grids also allows leveraging renewable energy resources such as wind and solar. However, from the perspective of cybersecurity, having a computer as the 'main brain' controlling a grid, brings along notable vulnerabilities in the loop.

Hawk *et al.* [30] provide an analysis of the cybersecurity aspect of the smart grid, along with a comprehensive explanation of the whole system, including the components of the smart grid. For example, considering the information technology (IT), and the operation technology (OT), which include the main controllers of the system, Hawk *et al.* emphasize the importance of including the cybersecurity aspect at the design stage and not after implementation. As such, security is taken into consideration when deciding to install and during the installation of the intelligent devices. Wazir *et al.* [31] provide a full analysis of the IEEE 33 bus system, which is actually the same test case as the one considered in this thesis. While this work is relevant [31], the conducted analysis did not include any cyber attacks. The main contribution relates to what could be the minimum loss of the system, or what could be helpful in order to have a good power flow of the distribution automation.

Batard *et al.* [33], provide an analysis of what could be a vulnerability in the smart distribution system, since the adoption of new control technologies using fast and wide-area communications, adds more restrictions in terms of cybersecurity. This work also provides a technical prevention scheme to avoid blackouts. In this context, the authors mention the use of backup and restore activities to prevent data loss. They also mention the use of secured communication protocols, the use of cybersecurity policies such as role-based access control (RBAC), as well as effective firmware upgrades on the equipment installed in the system. Lim *et al.* [34] provide an idea about applying security algorithms on some known cyberattacks against the distribution automation system. The authors also

provide relevant information about IEC standards designed for communication protocols, communication technologies, and the equipment used in distribution automation systems.

Among the mentioned communication protocols, IEC 104 and DNP3 are considered as secure and reliable for the distribution automation system. Lim *et al.* provide examples of cyber threats in the distribution automation system network, for instance, denial of service attacks that can make the collection of required measurements for different applications difficult, if not impossible, and then the applications would fail eventually. The other contribution of Lim *et al.* was in relation to the requirements for the distribution automation system security, which include: message confidentiality when collecting measurements of consumers and the availability of the measurements for applications or just for data collection. As for the security algorithms provided by Lim *et al.*, message encryption is mentioned along with the usage of message authentication code (MAC).

Another work that can help researchers to understand the cybersecurity aspect of the distribution automation system and its importance to have in such a system is published by Benoit *et al.* [36]. In this work, the authors define the cybersecurity requirements for distribution automation as well as the different actors in distribution automation systems, which include: the user, the maintainer, the central application, the field application, the control authority, and even sensors, which can have a role in distribution automation systems. Benoit *et al.* discuss as well a failure analysis of the distribution automation system with respect to 10 different objectives of the different roles in the system.

By achieving these 10 objectives, it is easier to secure the distribution automation system, since failing to achieve one of these objectives fails it will lead to system failure. Finally, this work also mentioned a security control scheme, which includes techniques to secure the network, the field devices, the security of the communication, etc. Hu *et al.* [38] discuss the usage of state estimation to detect false data injection attacks. The authors goal is to find vulnerabilities in a system under FDI, along with simulation examples showing

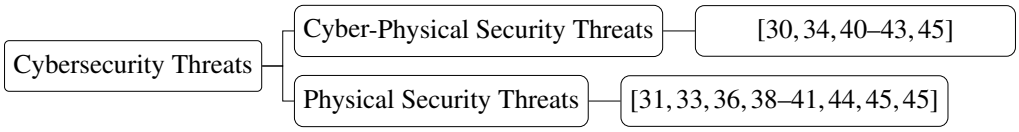


Figure 4: Taxonomy of Cybersecurity Threats.

the usefulness of state estimation algorithms in detecting this attack. Gunduz *et al.* [40] provide an analysis of cyber-attacks on smart grid applications. The authors describe real-life cyberattacks, such as the Stuxnet attack in 2011 [45].

In conclusion, cybersecurity is a very important aspect in distribution automation systems. It has to be considered at the design phase of the system and not after that. Moreover, the reliance on state estimation tools is not sufficient. Even a simple attack could lead to severe consequences such as blackouts, and physical damages to equipment in the field. Also, access to the distribution automation system should be restricted based on the role of the person or the component within this type of systems. Figure 4 illustrates the taxonomy of different cyber threats that the distribution automation system faces, either from a physical or a cyber-physical perspective.

3.3 Security Monitoring

One of the objectives of this thesis is to elaborate a security analysis approach suitable for distribution automation systems. In this context, we implement a security monitoring platform with a real IEEE test case, and execute simulated cyber attacks. Another objective is to implement and test the effectiveness of state estimation in detecting FDI attacks. Finally, we highlight the importance of deploying machine and deep learning techniques in order to efficiently detect attacks that the bad data detector (BDD) fails to detect.

We review next most of the recently published and prominent works that tackle anomaly detection in distribution automation. Then we classify these works based on the anomaly detection techniques implemented, whether it is a machine or a deep learning technique.

Ayad *et al.* [46] provide a formulation of the FDI attack on a radial 3-phase unbalanced system. Moreover, the authors study the IEEE 34-bus system as a test case for distribution automation system [46]. This work however only discusses a possible FDI attack formulation rather than detecting it.

Among the surveys conducted on FDI and related countermeasures for such attack on the distribution automation system, an interesting work is the recent contribution of Souhila *et al.* [2]. The authors discuss new ways to "bypass" the BDD shown in Figure 5 and describe two countermeasure techniques against bypassing the BDD: 1) detective and reactive, and 2) preventive. The authors also mention the usage of a "measurements-based detection technique" to detect cyber threats.

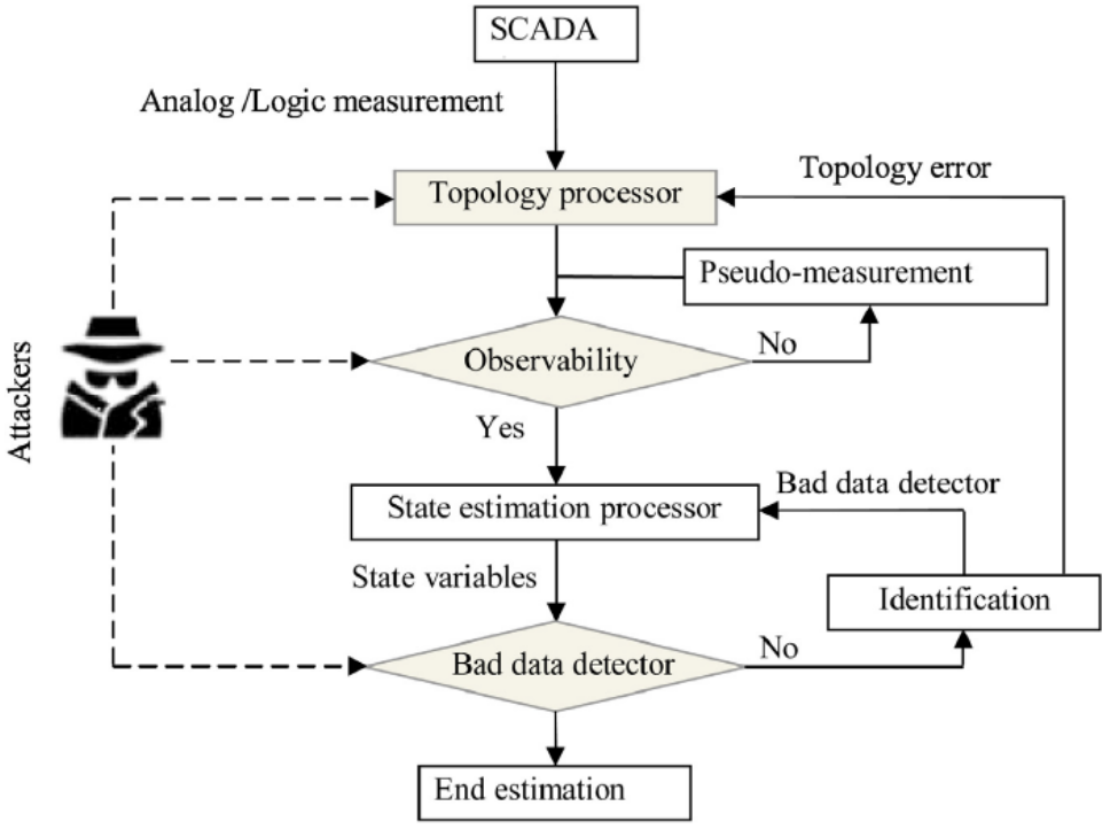


Figure 5: State Estimation Function [2]

Another relevant work is the one of Isozaki *et al.*, [47] where the aim is to detect cyber

attacks using a specifically proposed model other than machine learning techniques. The algorithm is meant to detect attacks against voltage control in the distribution automation system that has Photo Voltaic Arrays within the system. Although the authors do not mention whether the system has a state estimation implemented or not, the attack scenario is relevant to our research, since we are interested in all of the applications of the distribution automation system. The proposed algorithm is mainly rule based, which is traditionally one of the possible techniques suitable to detect anomalies. However a study by Soofi *et al.* [3] shows the limitation of traditional techniques and emphasizes the benefits of adopting classification techniques to detect anomalies.

The main contribution of this work is the usage of machine learning techniques for anomaly detection. Specifically, this work is focusing on classification techniques involving supervised learning in order to classify normal and abnormal data directly from the measurements. In this work, a list of possible classification techniques is mentioned, indicating those suitable to detect anomalies in different applications. Among the mentioned applications is distribution automation system data, as shown in Figure 6. The discussed techniques include Bayesian networks, Support Vector Machines, k-Nearest Neighbor, and different other techniques. As for the applications, several ones are given as examples, such as, electricity price prediction, telecommunication and internet networks, etc.

A similar work by Mohammed *et al.* [48] mentions four supervised machine learning techniques for classification, namely, k-NN, Decision Trees, Support Vector Machine, and Artificial Neural Network, which allow to detect anomalies. This comparative study also mentions the strengths and weaknesses of each technique and their areas of applicability. Another work by Osisanwo *et al.* [49] compares different supervised machine learning techniques. These techniques employ labeled data, whereby it is easier to classify normal and abnormal data in order to detect anomalies based on the nature of the measurement data itself [50]. Since it is likely that our data is similar to the data used in these different

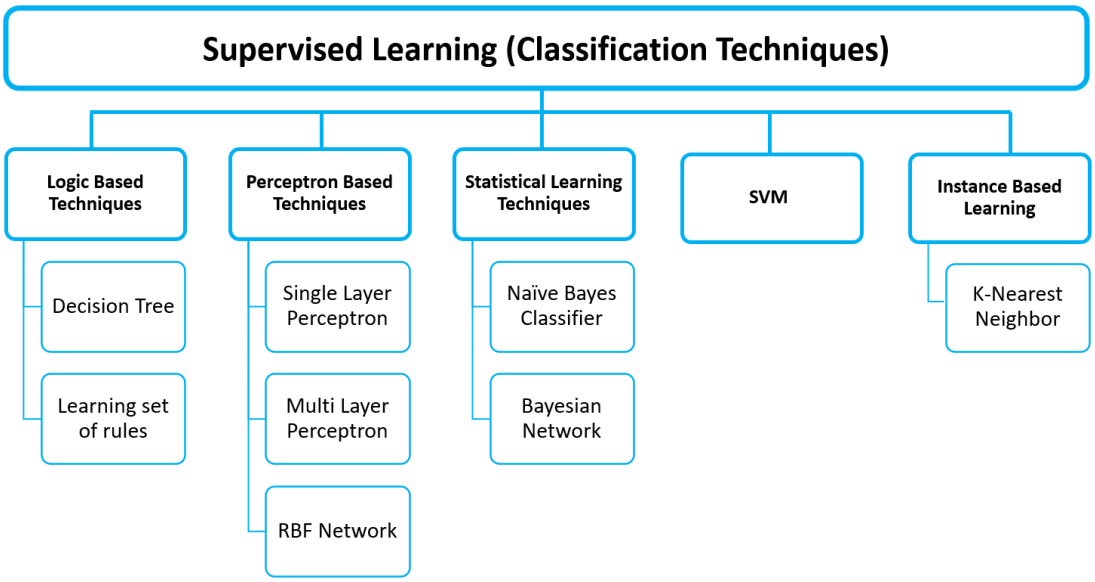


Figure 6: Supervised learning classification techniques [3]

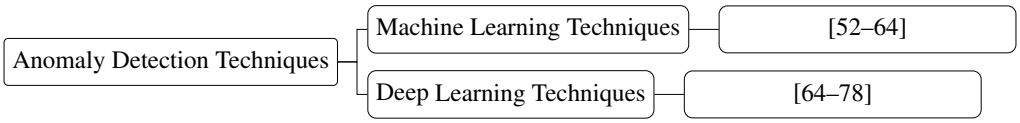


Figure 7: Taxonomy of Anomaly Detection Techniques.

studies, it is appropriate to consider the use of similar techniques for our data as well, although there is a lack of deep learning techniques usage in the anomaly detection case. However, we mention one particular work by Martinelli *et al.* [51] on power distribution system data where the authors use an Auto-encoder model to detect anomalies using one input layer, 3 hidden layers, and one output layer. Based on the reviewed works on anomaly detection, we can categorize the leading techniques. Then, we can pick the most promising ones to detect anomalies in our distribution automation system, as mentioned in the gap analysis section along with other relevant findings. Figure 7 contains the taxonomy of the anomaly detection techniques.

3.4 Gap Analysis

In this section, we identify the gaps after conducting the literature review. In terms of simulating the distribution power system, to the best of our knowledge, there is no published work that considers OpenDSS-G as a power simulator, even though it has numerous features for power distribution systems' simulation. The only work that discusses the use of this tool is provided by the developers who implemented it. With respect to the communication simulation in power distribution systems, we could not find any published work that mentions the possibility of emulating the communication network. Most of the reviewed works suggest simulating using OMNET++ or other network simulators.

As for the works discussing cyber attacks on distribution automation systems, the main objective was to find relevant works that could either target the network of the distribution automation system, or specific applications of the distribution automation system. Most of the reviewed papers discuss cyber attacks that mainly bypass the BDD. We notice only a limited number of existing works discussing attacks on different distribution automation applications. For anomaly detection techniques existing in the literature, different supervised machine learning techniques, mainly involving classification algorithms, were studied and the conclusion is that such techniques are suitable for detecting anomalies in distribution automation systems. However, we could not find relevant works that focus on using deep learning techniques on distribution automation systems with the exception of the work of Martinelli *et al.* [51], which uses Deep Auto Encoders.

To conclude, the existing techniques employed for the security assessment of distribution automation systems are not suitable to detect new and more advanced cyber attacks. As such, the commonly used anomaly detection techniques are not sufficient to detect these attacks. Therefore, we must implement new and effective detection techniques leveraging machine and deep learning algorithms. Based on our study of the most promising techniques, we find that the most suitable ones are the following: supervised machine learning

techniques to classify normal and abnormal data, and deep learning techniques for anomaly detection such as: Deep Auto Encoders, Long Short Term Memory, and Multi Layer Perceptron.

3.4.1 Supervised Machine Learning

Several techniques used to classify normal and abnormal data are investigated and reviewed in details in the following subsections.

Decision Trees. This is a popular technique for data classification [52]. It is named this way because of the decisions made by different trees. These trees decide the classification of the data based on certain features [53]. For anomaly detection, a decision tree would get the input values of the features of the data, and then the decision shall be either 0 for normal and 1 for abnormal based on the settings of the model itself. There are different types of decision trees such as: ID3 (Iterative Dichotomiser 3) [54] and C4.5 [55].

Bayesian Networks. The main usage of the Bayesian networks is for probability associations between a set of variables [56]. However, Bayesian Networks have a limitation when the attributes are continuous since they require discrete values. This means that the data is not fully used while learning due to issues relating to noise that might be introduced, missing information, and also consciousness to the change of attributes [56–58]. As for the advantages, Bayesian networks tend to be smooth while adding or modifying the properties, and have a possibility of using identical models to solve regression and classification problems [59].

k-Nearest Neighbor. This technique consists of finding the nearest neighbor by setting the value of k, which indicates how many nearest neighbors to consider for a record, and therefore classifying those neighbors as one cluster/class [60]. Among the advantages of

k-NN are the effectiveness in large data sets, where the scaling over huge amounts of high dimensional data is a feature of such technique [61, 62]. Other advantages of this algorithm are: the robustness to noisy data and the simplicity to understand and model. As for the disadvantages, this technique is computationally complex and has a poor run time performance [63].

Support Vector Machine. It is another technique that can be used as a supervised classification technique proposed by Vapnik [65]. The way the classification is achieved by SVM is by a hyperplane in high dimensional space [67]. Thus, it is suitable to classify high dimensional data [64]. The main advantage of SVM is to deal with a wide variety of classes, meaning not only binary classification but multi-class as well. As for the drawbacks of SVM, it requires parameter tuning to have better results, which can be time consuming [68].

3.4.2 Deep Learning

Deep learning techniques are used to recognize complex patterns in datasets. Among the possible use cases of these techniques is anomaly detection.

Artificial Neural Networks. It is a mathematical model that tries to replicate how the biological neural network works in recognizing patterns. An artificial neural network has three important requirements: multiplication, summation, and activation. Thus, the input data needs to be numerical in order to apply weighting, meaning that the data as an input is multiplied with a specific weight. Then, all of the weighted inputs are summed to obtain a bias. This bias is passed to an activation function to compute the output [69].

Auto Encoders. Another technique existing in the literature is Auto Encoders, which represents a deep learning technique that is used for dimensionality reduction [70]. The

latter is achieved by representing the raw data in a more compact way. The Auto Encoder consists of: an encoder, hidden layers, and a decoder. There are several Auto Encoder types: 1) Stacked Auto Encoder where it has more than one hidden layer stacked; 2) Sparse Auto Encoder where the hidden layers have the sparsity constrains; and 3) the De-noising Auto Encoder which removes the noise from the data [71].

Recurrent Neural Networks. The idea of this technique is to use the output alongside the input as well. This means a huge dependency between the output and the input [72]. Recurrent Neural Networks (RNN) are used for speed recognition and time-series analysis. There are two types of this technique: 1) Long Short Term Memory (LSTM) [73], where the input is a window of the data and then trying to predict the next window. 2) Gated Recurrent Unit (GRU) [74]. This technique is suitable recognize patters that have time dynamics.

Different Other Techniques. Other techniques, which are considered as deep learning techniques, can be used to detect anomalies. These include: Deep Belief Networks [75], Convolutional Neural Network [76], and Generative Adversarial Network [77]. However, we could not find published works that discuss using these techniques to detect anomalies in distribution automation systems.

Chapter 4

Methodology

In order to analyze the security of distribution automation systems, the most important step is to develop a realistic model together with the underlying automation applications in a co-simulation framework. In this regard, this chapter details the elaborated model along with the developed experimental co-simulation framework, as well as the telemetry data collection process. The security analysis of the collected data is detailed in the next chapter.

We start with the elaboration of a DAS model, which is an IEEE benchmark for a distribution grid. The model is validated and input into our co-simulation framework. Subsequently we add the control and protection layers to the developed system to enable the applications that are required for the proper operations of the distributed grid. In our co-simulation framework, we design, implement, and integrate typical and representative automation applications, namely fault localization isolation and service restoration, feeder reconfiguration, and voltage regulation.

The efficient deployment of these applications requires specific communication infrastructure that we implement in our co-simulation framework. It is important to mention that all the aforementioned layers are interconnected within our framework, which allows gathering telemetry data in near real-time.

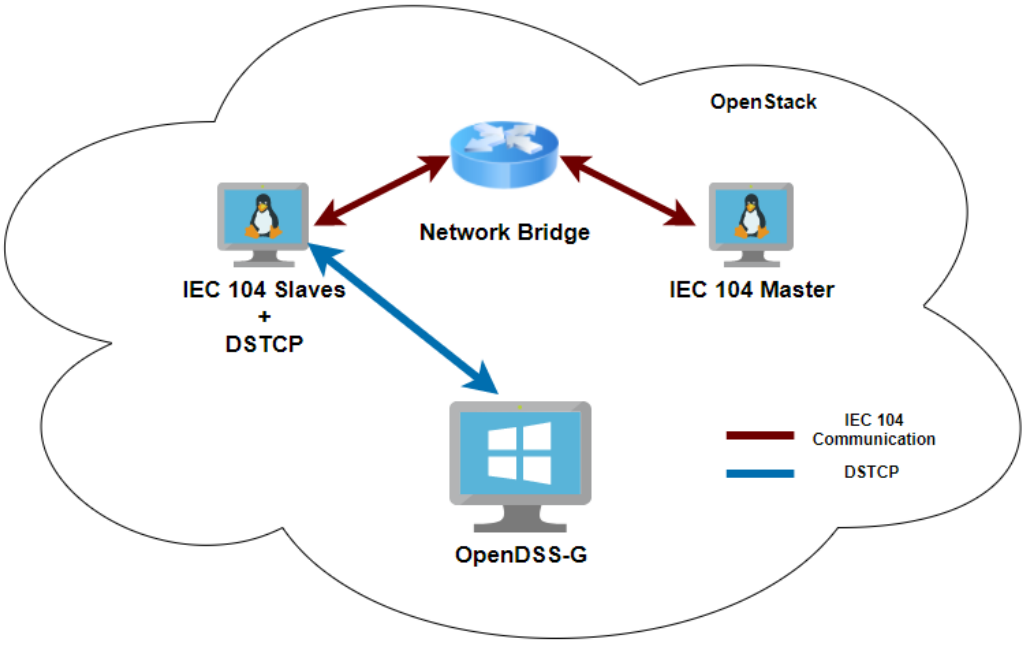


Figure 8: Distribution automation system's testbed

4.1 Power Model

In this chapter, the IEEE 33-bus system is used as the benchmark for distribution systems. The corresponding 12.66 kV distribution grid consists of 33 buses, 5 switches, 4 reclosers, a voltage transformer, a tap changer, and 32 loads. These loads, which represent the grid's consumers, can be industrial, commercial, or residential. To demonstrate the power consumption as a function of time, a load curve is utilized for each load of the system depending on the considered consumer type. In the normal operation, this power system is operated radially. As such, several of the tie-switches are in the open state. These switches get activated to change the feeder configuration of the whole network, or to clear out a fault that occurs in the system. This distribution grid is connected to the upstream transmission grid through a distribution substation.

The IEEE 123-bus system is used to prove the scalability of the proposed co-simulation platform. The IEEE 123-bus is a 4.16 kV distribution grid consisting of 91 loads, 6 reclosers, 2 transformers, and 4 voltage regulators. The same load curve is utilized for each

load of this benchmark.

The considered protection and control schemes composed of the voltage regulators and relays are used to identify faults and isolate them from the rest of the system. The reclosers are tripped in the case of an over-current directly resulting from the faults. In the distribution substation, the over-current relays protect the entire distribution grid in the event of a fault by tripping the corresponding circuit breaker. In such a case, the distribution grid is supplied through neighboring distribution substations. The control scheme of the distribution automation system is based on the voltage regulator. This regulator measures the voltage and changes the tap of the transformer so that the voltage remains within the desired range. Fig. 9 shows the general scheme of the distribution system.

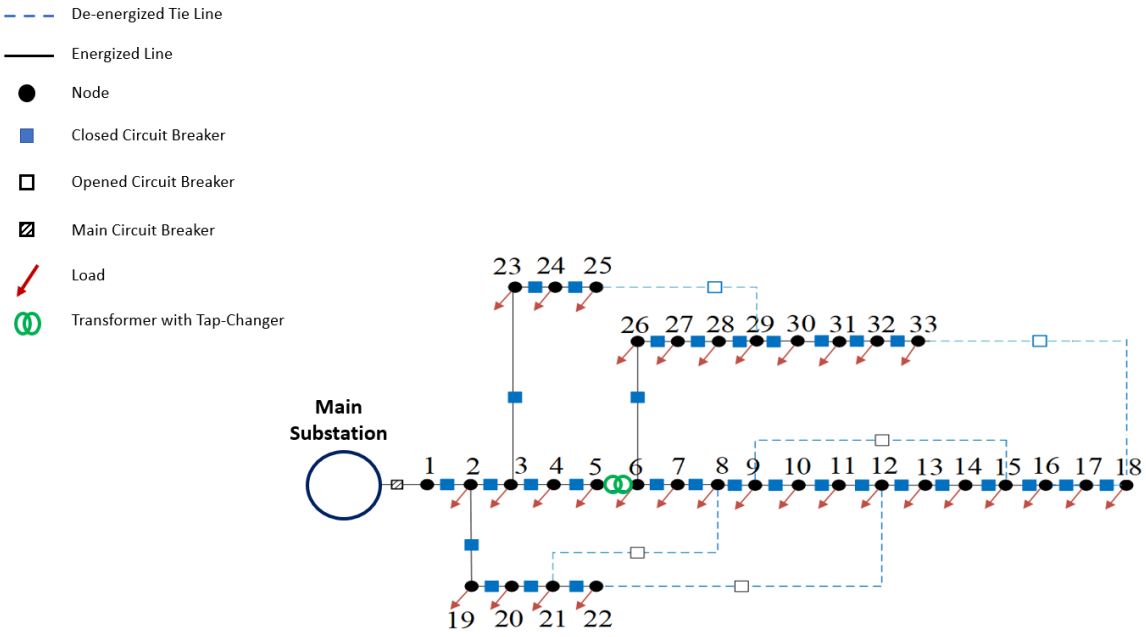


Figure 9: Power model of the IEEE 33-bus system

OpenDSS-G is used to simulate the power model. This software is tailored for distribution systems and contains all the functionalities required for the analysis of such systems. The software also provides a graphical user interface, contains different test cases, provides the ability to extract and collect data, and interfaces with the other software packages using

a specific data exchange protocol named DSTCP. Since we aim to build our framework based on data exchange, we translate the output of the DSTCP using a Python file. The IEEE 33-bus system is modeled in OpenDSS-G. Also, we implement a different version of DSTCP, specifically tailored for the implemented test systems.

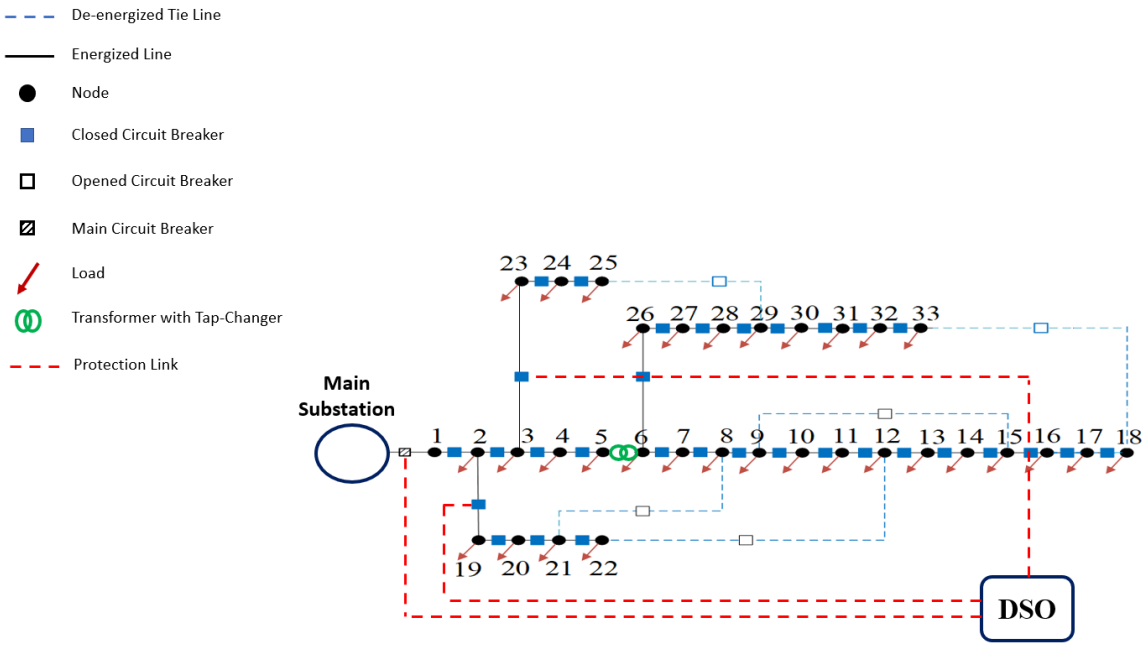


Figure 10: Protection layer of the IEEE 33-bus system

The deployment of protection and control layers requires proper implementation of the communication system along with reclosers, voltage regulators, and tie switches to maintain control over the system. Figures 10 and 11 illustrate the intended nodes and the communication schemes required for the protection and control layers, respectively.

4.2 Communication Model

A communication infrastructure is implemented in order to mimic the behavior of a smart distribution system where data is being exchanged among the nodes of the system. The

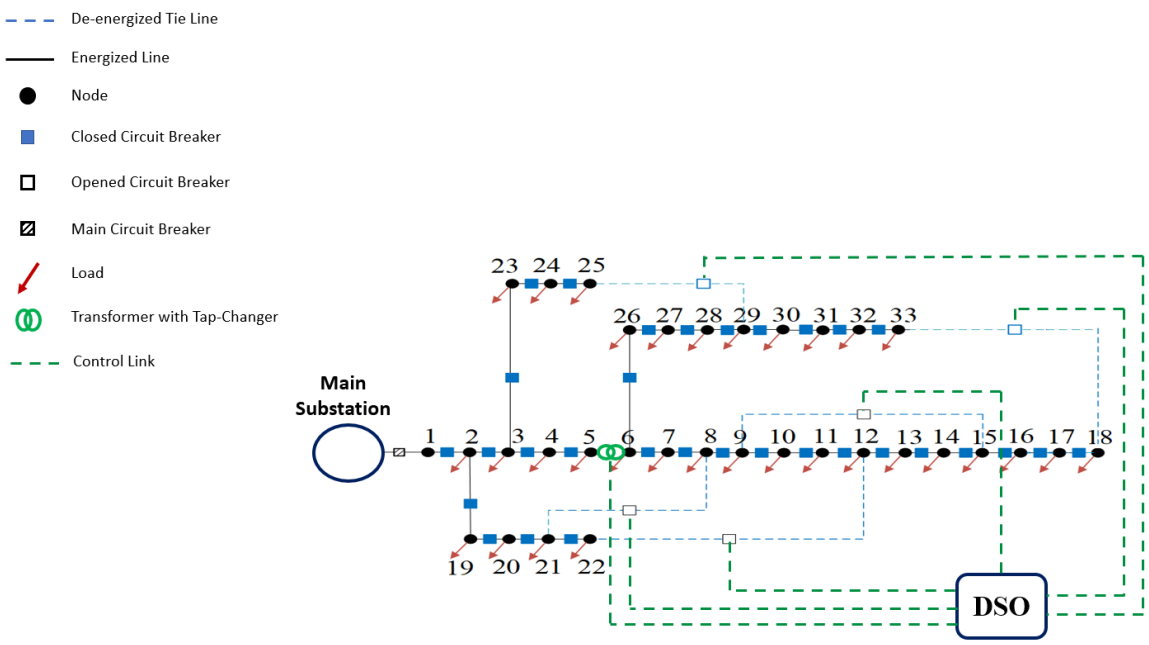


Figure 11: Control layer of the IEEE 33-bus system

data is a collection of different types of measurements: active power, reactive power, current, voltages, and state of reclosers and tie switches. After conducting the literature review to understand which communication protocols are used in power distribution systems, we determined that the most commonly-used ones are: DNP3 or IEC 104, and MODBUS. In this thesis, IEC 104 communication protocol is used due to its similarities with DNP3 and the availability of an open-source library for it. The idea of creating the communication infrastructure consists of virtual machines, and a software implementation of IEC 104 slaves for every node of the IEEE 33-bus system.

By a "node" we refer to all the previously mentioned components of the system: a load, a line, a switch, a recloser, and a tap changer. All these are considered as nodes since they are supposed to share data of specific types with one IEC 104 master. The master in our system is the distribution system operator (DSO). The advantage of using the IEC 104 protocol is the ability to host multiple instances of IEC 104 slaves on the same machine using different port numbers. Then, the IEC 104 master has an implementation of its own.

This implementation should contain all the information about which slaves the master is supposed to communicate with, what type of data or requests should it send, and what type of responses it is supposed to receive.

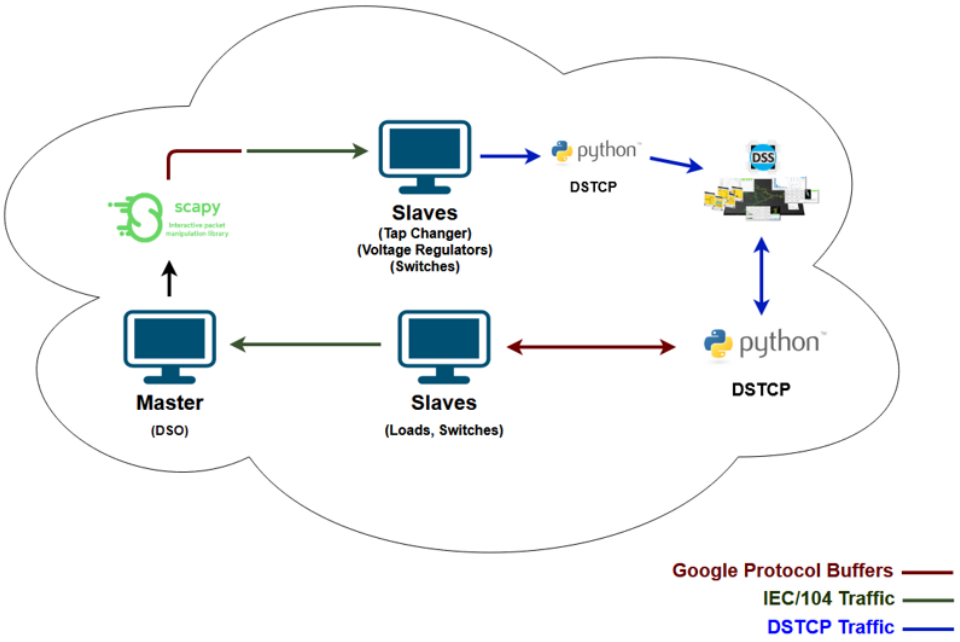


Figure 12: Proposed communication architecture

Since the only data exchange protocol that OpenDSS-G supports is DSTCP, the translation between the DSTCP and IEC 104 is implemented in Python. To this end, two virtual machines are created: the first one hosts the IEC 104 slaves, whereas the second one hosts the IEC 104 master. A specific IP address is given to IEC 104 slaves' machine. Then, a specific modified implementation of the IEC 60870-5-104 open source C library from Mz-Automation team is added and installed on this machine. The implementation of the code allows specifying which communicating nodes are involved, as well as specifying which port number identifies which slave. In addition, the implementation also defines the exact type of data and where does it originate from, as well as which data is supposed to be shared with the IEC 104 master.

A set of slaves is created such that all the nodes of the IEEE 33-bus system are considered as IEC 104 slaves. The second virtual machine is the IEC 104 master, which has a different implementation of the code that requires deep understanding of the open source library and each of its functions. The way that IEC 104 works involves the master sending requests to the slaves, based on the TypeID of the data. There are 127 different TypeIDs, each of which defines a specific type of data to be shared. Then, the slaves must have this list of TypeIDs mentioning the exact type of data that the slaves send. Based on this principle, the master communicates to the slaves accordingly. Another important point to check in order to make sure that we have the correct communication between each slave and the master, is to define the connections at the master side. The IEC 104 master initiates communication to each specified IP address corresponding to a slave device that supports IEC 104.

After adding all the connections of the IEC 104 slaves in the IEC 104 master code, we proceed to initiate the communication testing to evaluate the schemes that we develop. The next phase involves sharing the data, which is coming from the power system. Using DSTCP, we manage to collect in real-time the output of the power system as measurements and status of devices. While the data is collected in real-time, we cannot keep storing it in CSV or text files. Among the reasons why writing the data using DSTCP and then reading it using the IEC 104 code is not efficient, is the slow throughput. This means that the data exchange will happen but not in real-time (i.e., with a delay).

The requirement of IEC 104's data exchange rate is 4 messages per second. Therefore, we adopt a better solution, namely Google Protocol Buffers, which can sustain the necessary throughput. The idea is to implement the Google protocol Buffers such that two nodes are talking to each other. One node sends data that can be intercepted by another node without compatibility issues. This method allows to exchange input/output data

between different programming languages and represents a typical use case of Google Protocol Buffers. Similarly, we have a data exchange tool between Python DSTCP and IEC 104 written in C code. The idea is that DSTCP is collecting measurements and stores the data into the buffer, using the data exchange tool previously mentioned. Then, the IEC 104 slaves are awaiting to read any data in the buffer. For example, load 2 could read the data that is intended for load 4. To prevent this from happening, we specify the data by load identifier. A significant benefit of Google Protocol Buffers is that the data exchange across all the nodes storing data completes within 220 milliseconds, compared to a total of 7.4 seconds needed when using text or CSV files.

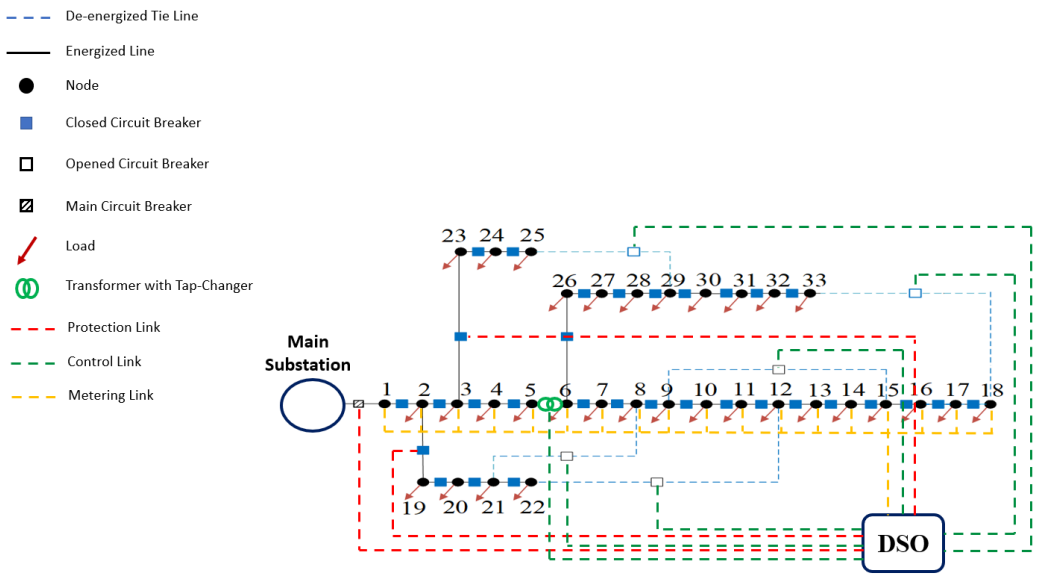


Figure 13: Communication model of the IEEE 33-bus system

We test the smoothness of the communication where the data exchange should be in sync with the power system's output. The collected results show that no piece of data is dropped or missed.

In conclusion, the communication model consists of different pillars, working in conjunction to ensure the realistic communication emulation of the automated distribution system, as well as its functionalities and applications. Our communication model emulates the

network instead of simulating it. This ensures the realism of our co-simulation framework. Actually, based on what the IEC 104 standard states, all the data is being exchanged at the fastest transmission rates possible, which is 4 messages per second.

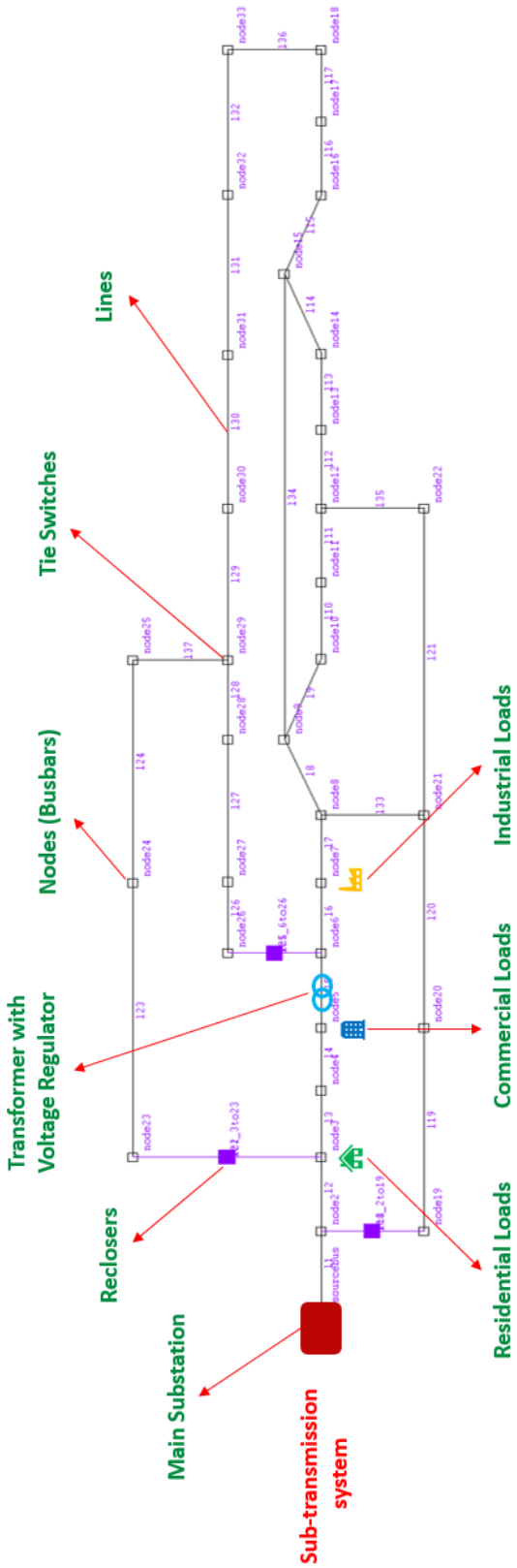
4.3 Implementation of DAS Applications

Benefiting from the developed communication infrastructure, we implement four major and well-known applications for automating different aspects of the IEEE 33-bus system. These applications are: (1) fault localization, isolation, and service restoration (FLISR), (2) feeder reconfiguration, (3) voltage regulation, and (4) bad data detector. Each of these applications is described in the following subsections.

4.3.1 Fault Localization, Isolation, and Service Restoration

In this application, the end goal is to locate and isolate the faults that occur in a distribution system, and restore the functionalities of the system accordingly. Using MATLAB and Python, this application is implemented. The operation of the application is validated by imposing different faults on the system. The output of the application is the correct location of each fault, and a set of open/close commands to the switches that isolate these faults, and allow the restoration of the service to consumers. Using DSTCP from OpenDSS-G, we are able to collect the values and send the data to MATLAB. Then, MATLAB allows to calculate the optimal configuration to restore the system to the normal operating conditions. This involves: disconnecting the faulty lines, opening of four other lines, and closing the tie switches.

Figure 14: IEEE 33-bus system implemented in OpenDSS-G



4.3.2 Feeder Reconfiguration

This application aims to reduce the loss in the system by opening the tie switches and changing the topology of the system based on the calculated loss. Initially, the operator calculates the loss at each line of the grid and the total loss of the distribution system by using the data received through DSTCP. Then, this application determines the new topology of the system by energizing/de-energizing different lines of the system, while ensuring that power is delivered to all loads.

4.3.3 Voltage Regulation

In this application, the input represents the voltage measurements that are collected using DSTCP from the co-simulation framework. These measurements are then transmitted from the slaves to the master, using IEC 104, and are intercepted by the translator Scapy. However, since no small generation unit is placed at the distribution system, the voltage measurement at the end of each lateral is sufficient for voltage regulation. By simulating the IEEE 33-bus system, we know that loads 18 and 32 are the end nodes with minimum voltage in the default configuration and loading of the system. After extracting the voltage values of the end nodes, we run a test to check if the values are above or below the thresholds. Based on that, we initiate a control signal to a slave named the tap changer with a gradual increase or decrease of the tap number until the voltage values of the end nodes are within the acceptable limits.

4.3.4 Bad Data Detector for IEEE 33-Bus System

One of the commonly-used applications in power systems is state estimation. This application allows the detection of bad data within the system. This estimation technique gathers the information periodically from the available measurements, such as, voltage magnitude

of the buses, active power, reactive power of the lines, etc. Then, leveraging the gathered data, the rest of system parameters are calculated by the operator. The selection of the number of measurements necessary to have a valid state estimation can be obtained using Equation 1, where n is the number of buses [79] and k is the number of slack buses. In our case $n = 33$, as we are implementing the IEEE 33-bus system and $k = 1$, since one slack bus exists in this benchmark.

An accurate state estimation depends on several inputs. These include the availability of a sufficient number of measurements and an appropriate accuracy of the algorithm. The state estimation technique that we are using in our modeling is based on the PandaPower tool and the weight least squares (WLS) state estimation algorithm [79].

$$m_{min} = 2n - k \tag{1}$$

The state estimation also needs another parameter, which is the standard deviation. In any power system, it is commonly known that there are errors in the measurements due to noise or various kind of bad data. Therefore, the standard deviation is considered to be the margin of error for the measurements. The standard deviation is either 1% for voltage magnitude values, or between 1% to 3% for the other type of measurements, which could be the active/reactive power and current [80].

The implemented bad data detector operates based on a residue function. This function is evaluated by comparing the measurements received from the system against those provided by the mathematical model. A residue more than a specified threshold creates an alarm regarding the bad data detector. The main challenge while building this detector is to determine the value of the threshold. The selection of this value has a significant impact on the security analysis in FDI attacks since an attacker who alters the measurements while keeping the residue below the bad data detector's threshold will remain stealthy.

4.4 Distribution Automation System Testbed

The distribution automation system co-simulation framework consists of two parts: a real-time power simulator, and a communication network emulator that uses the IEC 60870-5-104 as a communication protocol for data exchange. The data that is used and communicated among the nodes of the system is generated directly from the power system simulator of the distribution automation system. We do not use only the power simulator and the communication framework, as they are technically separate due to interoperability issues of different software, tools, etc. However, in order to achieve data exchange in real-time, we use different input/output tools that ensure the reading and writing of the data in real-time between several devices without significant demand of computational power. We note that, to the best of our knowledge, our testbed is a first systematic attempt to develop a co-simulation framework for distribution automation systems. The co-simulation framework allowed gathering real data in real-time, and using fast input/output techniques.

All the power system models, distribution automation system applications, and communication infrastructure are orchestrated together in the co-simulation testbed, which is a combination of three different virtual machines. The first one is a Windows machine that has OpenDSS-G installed on it since OpenDSS-G is only compatible with Windows operating system. The second machine runs on Linux, and it hosts the DSTCP implementation in Python, and the IEC 104 slave implementation written in C code. DSTCP and IEC 104 must be running in sync on the machine. The third machine runs also on Linux, and hosts the IEC 104 master implementation also written in C code. The implementation of DSTCP contains the Python code that has our version of this library developed using the open source and fully modifiable original library from the developers. In the Windows machine, while building the IEEE 33-bus test case, we create the system from scratch using OpenDSS-G. The IEC 104 code for the slaves is taken from the Mz-Automation communications library, which is open-source and available to download and modify.

The Mz library is upgraded to have a full communication network of the IEC 104 protocol itself for all the nodes of the IEEE 33-bus system. It is safe to mention that one machine is capable to handle all the nodes. Instead of using different machines, we use only a single one capable to handle the fully communicating devices using a simple change in port numbers. This is possible since the IEC 104 master can either distinguish the devices it communicates with using port numbers or IP addresses. The IEC 104 master's machine that contains its code is setup such that it includes: (i) the port numbers of all the communicating devices that it must connect with, and (ii) the types of data it is supposed to receive based on a periodic request that the master sends to the slaves at a rate of 4 messages per second. The whole network communication is TCP/IP and is designed in OpenStack.

Finally, for the data collection and the anomaly detection phases, we add another virtual machine using OpenStack and make it a bridge between IEC 104 slaves' machine and IEC 104 master's machine. This structure allows us to have more control over the network itself, by observing every packet. The bridge also allows us to collect the data accurately, and can even serve as the point of initiating simulated attacks since it can act as a man in the middle. The machine that we use for anomaly detection has a RYZEN 7 3700x processor with 16 cores @ 4.4 GHz, 64 GB of RAM, and Nvidia RTX 2080Ti GPU with 4352 CUDA Cores. Moreover, we use elastic-search as a database for data collection and further analytics. We use Kibana to design the distribution automation system dashboard for data visualization in a fashionable manner. Also, we use Grafana to achieve more control over the dashboards since it is the more customizable open-source version of Kibana. Finally, we design our own dashboard to control the distribution automation system. Our dashboard allows to check the connected devices, to inspect the status of the switches and reclosers, and to view the measurements in real-time. Moreover, it provides the possibility to execute simulated cyberattacks.

4.5 Simulated Scenarios

In order to understand the dynamics of a real power distribution system, several demonstrative scenarios are simulated. For example, a normal application, a fault occurring in the system, and even attacks within the system. All of these scenarios are used to assess the behavior of the DAS under different conditions.

The normal operation of a system takes place when it is operating without faults and all its parameters are in an acceptable range. The execution of the applications that are supposed to ensure the automation of the DAS is also considered. Among the applications that we mentioned previously, the fault localization, isolation, and service restoration, the feeder reconfiguration, and the voltage regulation applications are the ones considered and simulated.

4.5.1 Faults Occurring During Operation

Faults can occur due to many reasons such as natural events, or human errors. For this scenario we are using OpenDSS-G to generate all sorts of faults within the system. There are several types of faults that can be implemented within OpenDSS-G directly, for example, 1-, 2-, or 3-phase to ground faults. Such faults, if not detected and removed properly, can result in very low voltage levels and extremely high current levels that can endanger the system components.

Chapter 5

Experimental Results and Analysis

In this chapter, we discuss the details of the threat model, attack formulation, datasets, and the detection techniques. The data collection phase is also discussed in details. Furthermore, we demonstrate the effectiveness of our attack detection techniques, which include supervised machine learning and deep learning algorithms. Finally, we compare and evaluate the proposed detection techniques based on their performance.

5.1 Threat Model

Our focus is on False Data Injection (FDI) attacks. However, we also consider the malicious dropping of packets as a potential attack in our threat model. We assume that the attacker has full access over the network by stealing credentials, or by compromising a device in the field. Compromising a device in the field can occur by infecting a device ahead of deployment via its supply chain, or by embedding a malware within a legitimate device (e.g., during firmware update). Thus, an adversary would be in a favorable position to carry out an attack in this context. We assume that security is implemented on top of the IEC 104 protocol. The security implementation of the IEC 62351-5 is available and would make an attack more difficult. We consider the implementation of TLS from the IEC

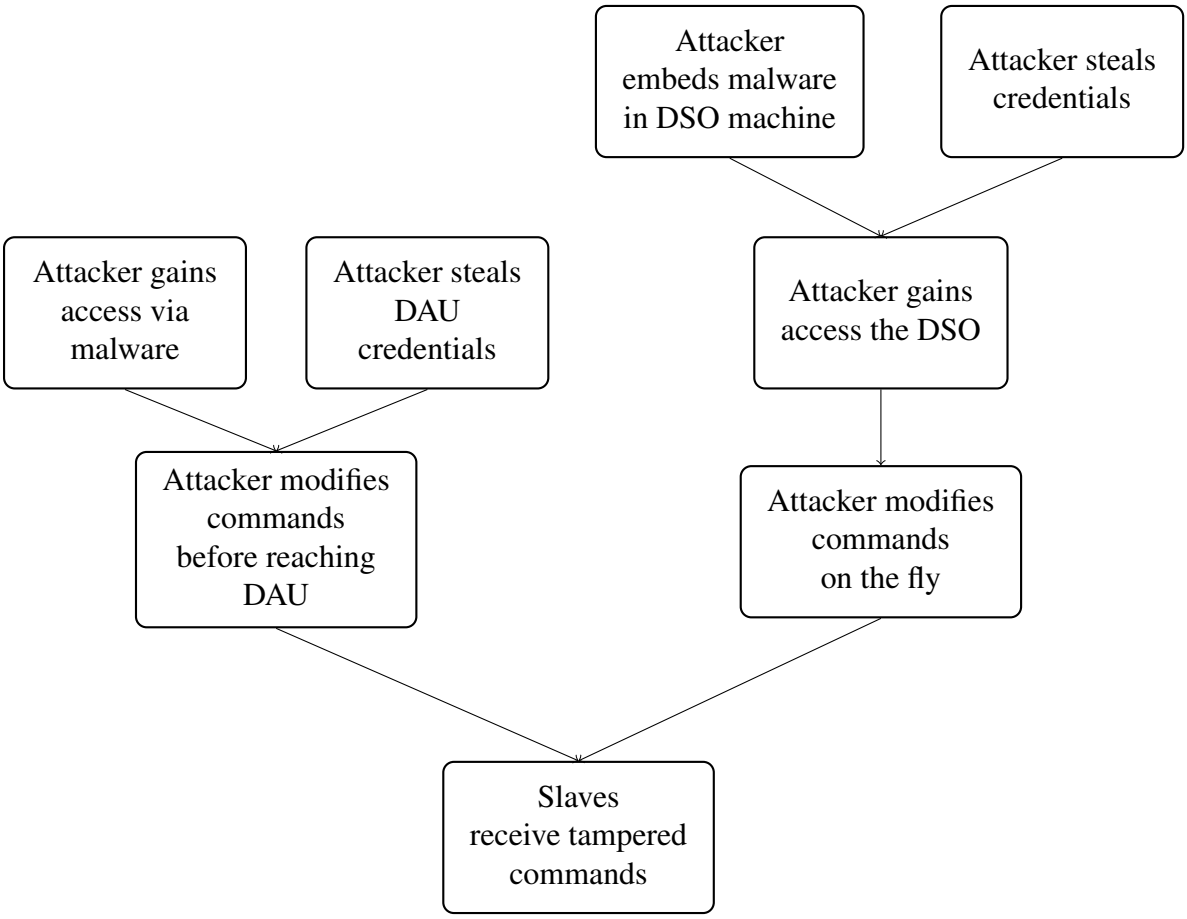


Figure 15: Commands Modification Attack Tree

62351-5 security protocol. However, since we are assuming that the attacker can control a rogue device or get access to one of the legitimate devices in the field, then the attacker can have access to the encryption keys. Therefore, the attacker is able to read packets in the clear. As such, we need to consider all valid assumptions under which an adversary could successfully carry out an attack. Moreover, we also have to consider the presence of various security layers, how they could be breached, and the impact on the power system's performance. Figures 15, 16, and 17 detail the different attack scenario.

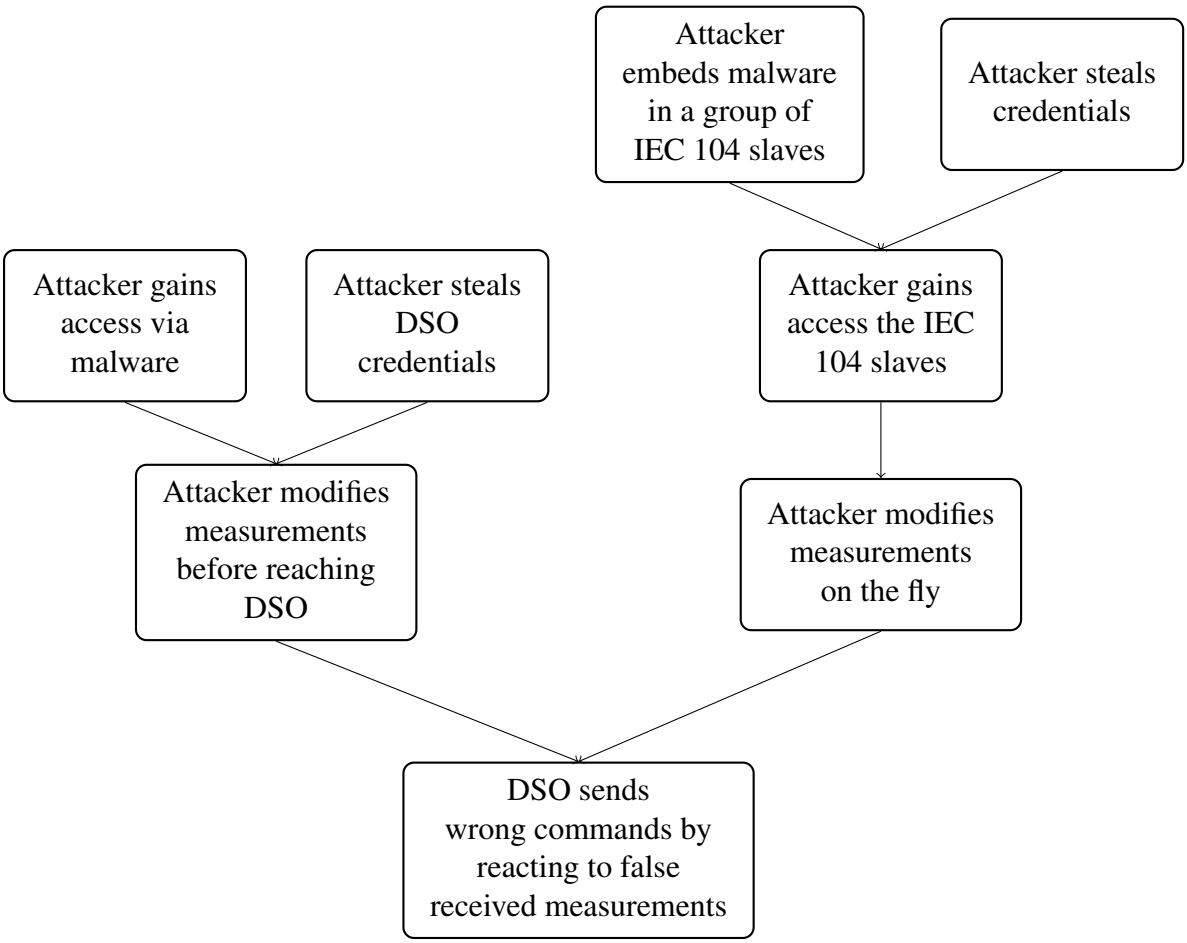


Figure 16: Measurements Modification Attack Tree

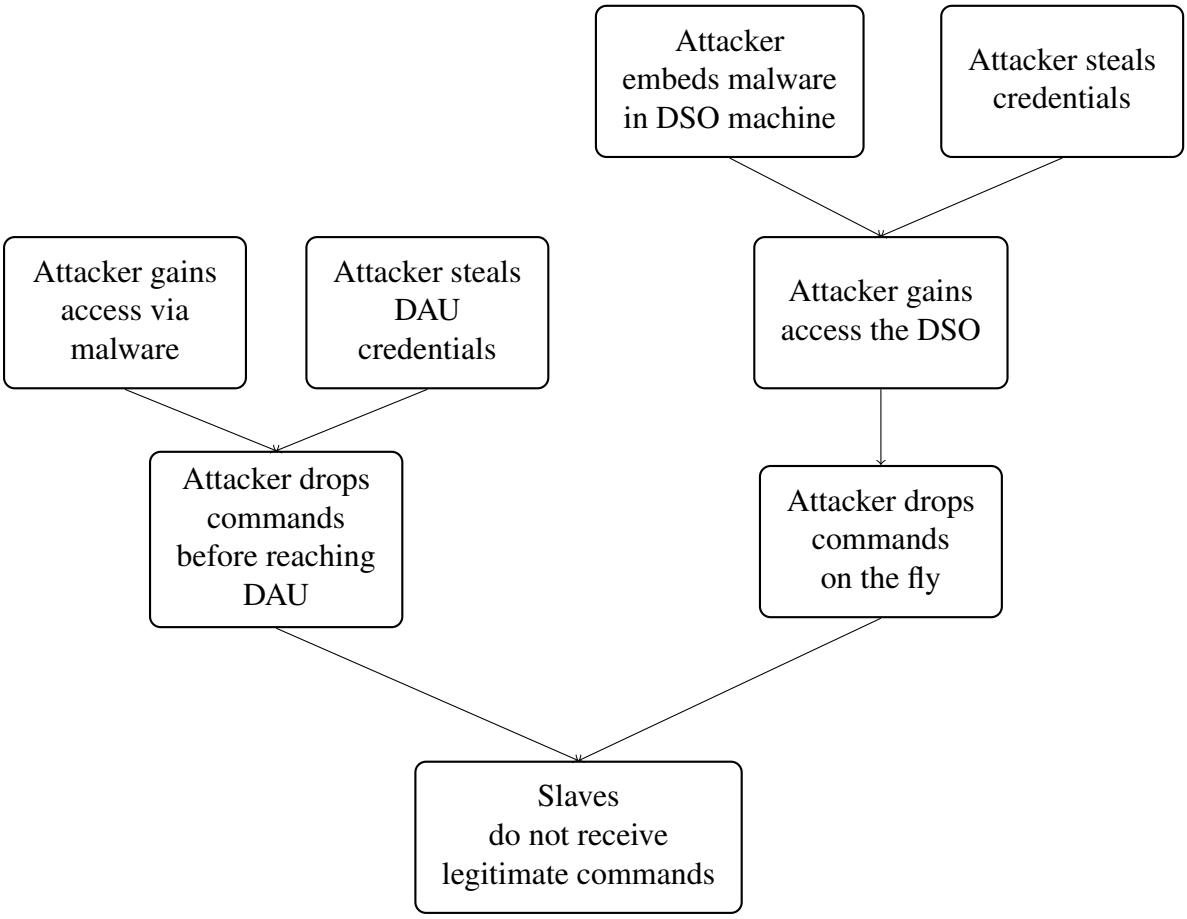


Figure 17: Commands Dropping Attack Tree

5.2 Attack Formulation

In our case, we assume that a knowledgeable attacker has full control over the distribution automation system. In other words, the adversary has access to any type of data since he/she can intercept packets, modify, delay, drop, and even inject new packets in the network. In this chapter, we consider that the attacker already bypassed the conventional security techniques (e.g., firewalls, network intrusion detection systems). This security layer can be breached using a malware, for instance, due to social engineering or human error.

In the attack generation step, we also consider the attacks targeting the IEC 104 communication protocol by exploring the vulnerabilities within the protocol itself, whereas the other attacks considered are those against applications of the distribution automation system. Thus, in this section we provide the general information on all the attacks that we implement in our testbed. We consider two attack classes: false data injection attacks, and dropping packets. Examples of these attack classes are then applied on distribution automation applications.

5.2.1 Attack Classes

False Data Injection Attacks

The intention of the attacker is to inject malicious commands or measurements in the network by either: 1) intercepting a legitimate packet and modifying the payload, or 2) by crafting a new packet containing the desired command or measurements. The attacker is able to carry out this type of attacks given the assumption that the DSO machine is compromised. However, this attack is also possible if one or a group of slaves are compromised. In this case, the attacker can modify or inject malicious packets from the slaves. Then, the DSO will react differently based on the received malicious packets. This attack tends to be stealthier than compromising the DSO.

Dropping Packets

In this type of attacks, the adversary is controlling the DSO machine, which allows the attacker to monitor the sent/received packets from this machine. The attacker can drop any packet coming from the IEC 104 slaves to the DSO, or he/she can drop a legitimate packet going from the DSO to the IEC 104 slaves. The goal is to prevent measurement values or status information from reaching the control application running on the DSO, or to prevent sending commands to the IEC 104 slaves.

5.2.2 Attacks on Distribution Automation Applications

As previously mentioned in Chapter 4, several applications within the distribution automation system are implemented in our testbed (i.e., fault localization, isolation, and service restoration; voltage regulation; and feeder reconfiguration). In this subsection we specify what could possibly go wrong if a malicious and knowledgeable adversary compromises the system and executes the types of attacks we are considering.

Attacks on FLISR

These attacks aim at targeting the FLISR application of the distribution automation system. The attacker awaits the occurrence of a system fault in order to intercept the packets containing the instructions for the isolation procedure. The procedure involves: 1) sending tripping commands to isolate the faulty line, 2) sending tripping commands to open 4 other lines based on the faulty line, and 3) sending tripping commands to close the tie switches.

In this context, the attacker intercepts the packets containing the tripping commands and can either: I) modify the header information to change the intended destination, or II) flip the binary value(s) of one or multiple tripping commands (close to open or vice versa).

Attacks on Feeder Reconfiguration

Similar to the attacks on FLISR application, the attacker awaits the occurrence of the feeder reconfiguration. The goal of the feeder reconfiguration application is to optimize the power loss in the system by sending instructions for the new PDS's configuration. These instructions correspond to tripping commands sent to specific tie switches in the system. In this situation, the attacker's goal is to intercept the packets containing the tripping commands. The adversary can then: 1) modify the destination port, or 2) flip the tripping command. The impact of this attack on the system is a significant power loss.

Attacks on Voltage Regulation

With respect to voltage regulation, we consider two different types of attacks. The first one targets packets that are sent from the slaves and are destined to the master, which contain the voltage values at the end nodes (e.g., nodes 18 and 33 in the IEEE 33-bus system). The attacker intercepts the packet and either increases the measurement values drastically or decreases them. The DSO, after receiving the false measurements, would react based on the intention of the attacker. The DSO sends a command to the tap changer to decrease or increase the tap number at the transformer level. This would decrease or increase the voltage for the whole system. Such an increase or decrease will push the system toward its operation limits until the protection system reacts and disconnects the impacted sections of the system.

The second attack takes place when the slaves report the correct values of the voltage at end points, and the DSO sends a command to increase the tap number or decrease it based on the received measurements. The attacker intercepts the packets that contain the tap changing command. The attacker will then cause the tap changer to increase instead of decrease the tap number with the intention to push the system toward its operation limit.

5.3 Datasets

During data collection phase, we use the bridge machine from the testbed. We collect IEC 104 data for training, testing, and validation. The collected data contains the messages exchanged between the IEC 104 slaves and the master that is implemented in the testbed. The messages can be: (i) measurements, (ii) status, and (iii) commands. The measurements are: active power, reactive power, voltage, and current values. The status values for tie switches and reclosers represent binary values. The command messages are the ones sent from the IEC 104 master to the slaves. These commands can either be tripping commands to the switches or the reclosers, or they can be tap changing commands. The data sampling rate is 42 messages per second. The simulation is following a yearly load profile set within the simulation phase, and the data is collected during the simulating and stored in the form of PCAP files. The PCAP files are eventually converted to CSV files. We validate the collected measurements with the corresponding output of the power simulator we have in the testbed.

In Figures 18, 19, 20, and 21, we can see an example of collected measurements for load 3. These measurements are validated by comparing them to the output of the IEEE 33-bus system. The aforementioned figures show the measurements for only the first 7 days.

The collected data represents 365 days of simulation, resulting in 8760 rows of measurements for all the loads. This allows having measurement data that account for seasonality variation across all four seasons.

5.3.1 Feature Extraction

The data collected from the testbed is a PCAP file corresponding to 365 days of simulation. This file contains the data exchanged between the IEC 104 slaves and the master. Based on our setup, these represent the devices connecting on port values ranging from 2405 to

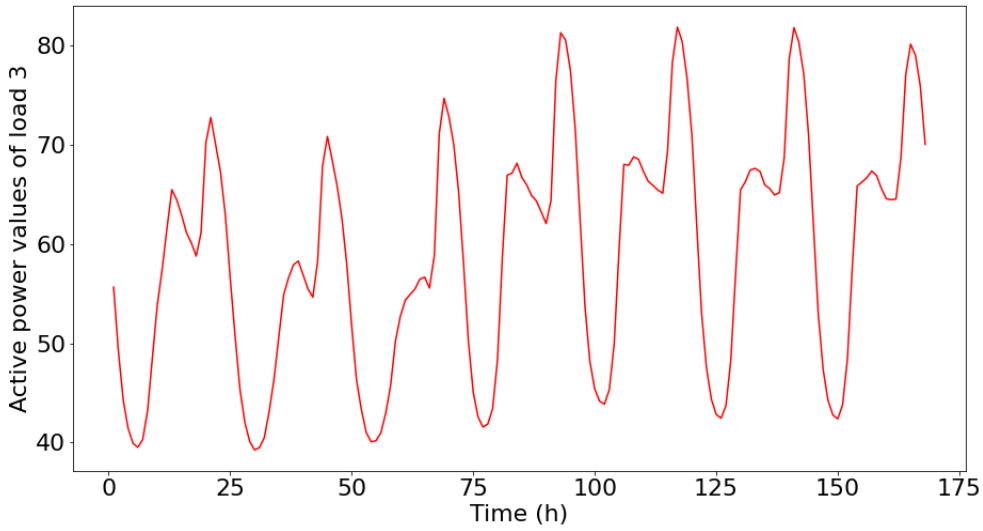


Figure 18: Active power measurements for load 3

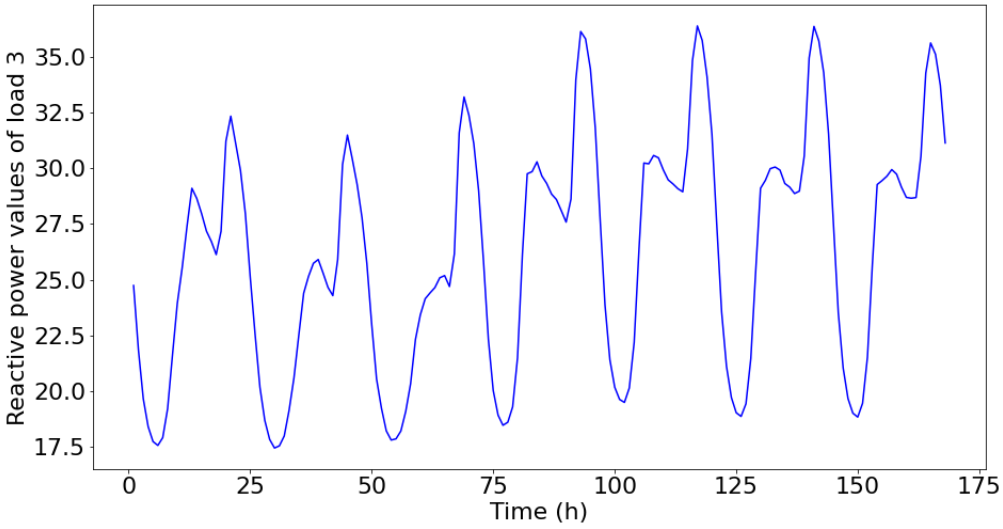


Figure 19: Reactive power measurements for load 3

2447, which correspond to: the 32 different loads, the 5 reclosers, and the 5 tie switches in the system. The DSO is communicating on port 2404. The extracted features are from the payload in these PCAP files. We clean the data by removing the status features as they contain lots of null values. The final features list includes the values of: active power, reactive

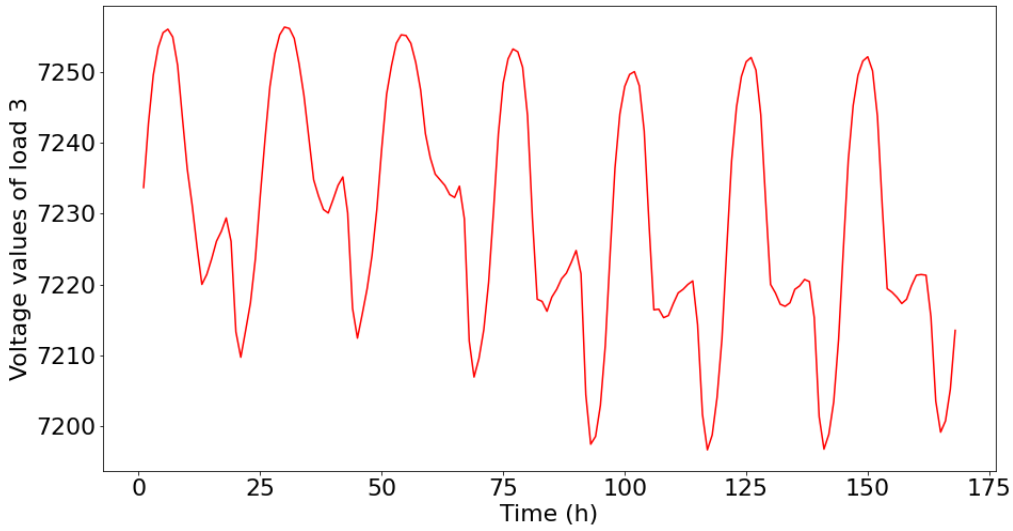


Figure 20: Voltage measurements for load 3

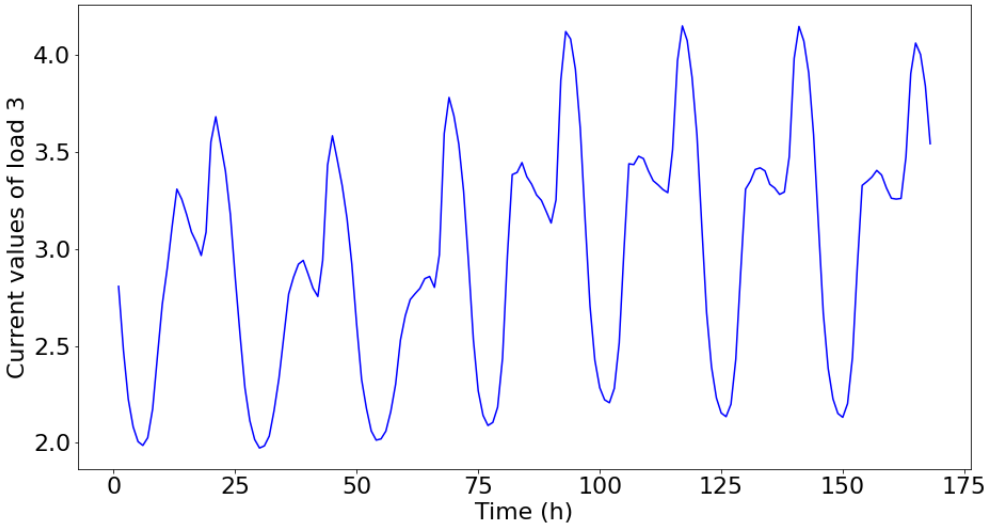


Figure 21: Current measurements for load 3

power, current, and voltage. We label the datasets based on the scenario occurring during that data collection period. These scenarios include normal labelled traffic corresponding to the normal behavior of the system , and abnormal labelled traffic corresponding to the behavior of the system during faults or attacks.

5.4 Detection Techniques

The bad data detector of the state estimator allows to detect some attacks, but it is not suitable for all types of attack scenarios. Therefore, implementing other detection techniques is helpful in detecting several anomalies that the bad data detector would deem as normal. These detection techniques can be implemented with the help of machine learning or deep learning algorithms. In Chapter 3, we reviewed several detection techniques already used for labelled datasets similar to our own. Thus, it is feasible to implement anomaly detection techniques based on supervised machine learning and deep learning algorithms.

5.4.1 Machine Learning Algorithms

From the literature review, we conclude that five of the top and most commonly-used machine learning algorithms are suitable for our datasets. These are: XGBoost, Random Forest, k-Nearest Neighbour, Support Vector Machine (SVM), and Decision Trees. The aforementioned algorithms are among the best for binary classification. These techniques allow for both rapid training time and fast response time to detect anomalies.

5.4.2 Deep Learning Algorithms

The idea of using deep learning techniques is to see if they outperform the previously mentioned machine learning techniques. Therefore, we consider using different deep learning algorithms to detect the anomalies and the attacks that can occur in our system under the different scenarios that we are considering. The corresponding models are: Deep Auto Encoders (DAE), Long Short Term Memory (LSTM), and Multi Layer Perceptron (MLP). A notable advantage of deep learning techniques consists in their ability to handle datasets with a higher dimensional feature space. In our case, our datasets consist of 128 features.

5.4.3 Hyper Parameter Tuning

Hyper Parameter Tuning, or in other words, adjusting the parameters of the model to have better results is an important step in deploying the deep learning techniques. Different parameter settings could lead to better results or sometimes worse. Therefore, we explore different optimizers and activation functions. Figures 22, 23, and 24, illustrate the different results obtained with different settings. For DAE, we start from 1 hidden layer, 3, 5, 7, until reaching 9 hidden layers, while having one input and one output layer. As for the activation functions, we try *Tanh*, *Relu*, *Selu*, *Sigmoid*, and *Elu*. We focus mainly on LSTM and DAE to experiment with parameter tuning. For MLP, the default parameter settings are considered. Thus, we select a specific set of settings, corresponding to a set of 3 multi layers (each of these sets has 13 hidden layers) and using the *Relu* activation function. We also tried different activation functions for MLP, but *Relu* provided better results.

As shown in Figures 22, 23, and 24 we can notice that for Deep Auto Encoders, the best results in terms of reconstruction error is achieved when using the parameters of 9 hidden layers, and the activation functions *Tanh* and *Elu*. As for LSTM, the goal is to predict the next window of the data, by taking a window of 60 values of the data, and trying to predict or reconstruct the next 60 values. Then, the predicted values are compared to the actual values in order to assess the performance of LSTM. As for the activation function, *Selu* tends to provide better results for LSTM compared to the other activation functions.

It is important to note that in LSTM we can easily set a threshold to make the model less sensitive to data changes. This allows the model to provide better results in the end, thus avoiding an increased number of false alarms. Another technique is used to better understand whether the parameters we are setting are adequate to obtain enhanced results during the testing of our model. We use *Tensorboard* to monitor the performance of the mentioned algorithms relative to the different hyper parameters we are using. In Figures 22, 23, 24, 25, 26, 27, and 28, we can see for DAE and LSTM the model performance

for different activation functions. With respect to the dataset, we are using a larger one that has 20,000 records, which are used as follows: 16,000 records for training while 4,000 records are used for validation. This datasets is collected from the testbed in order to obtain a larger number of records, given that deep learning models such as LSTM perform better when they are trained on large datasets. The number of epochs is 100 and we are using CUDA from Nvidia to get the results quicker.

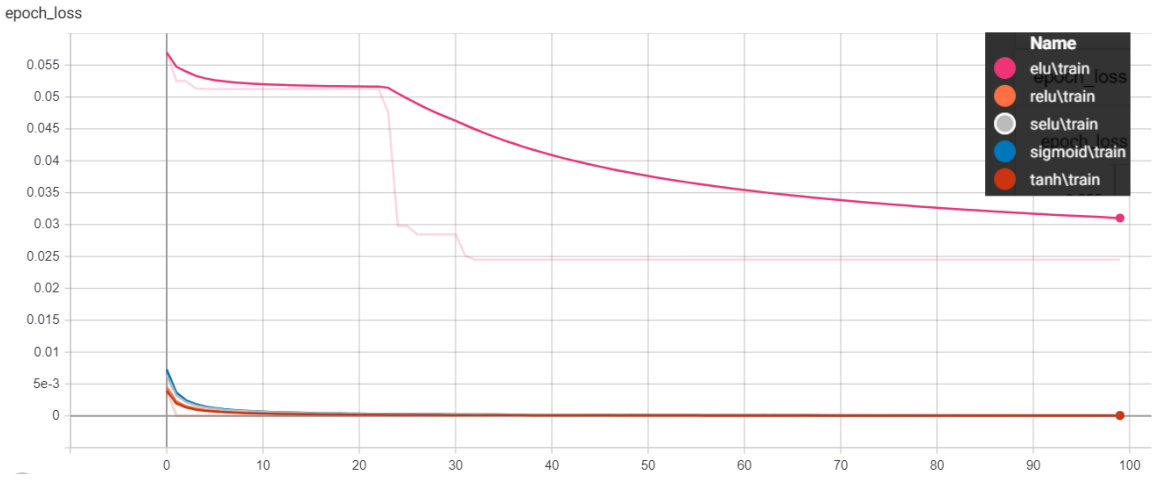


Figure 22: DAE: loss values (3 hidden layers)

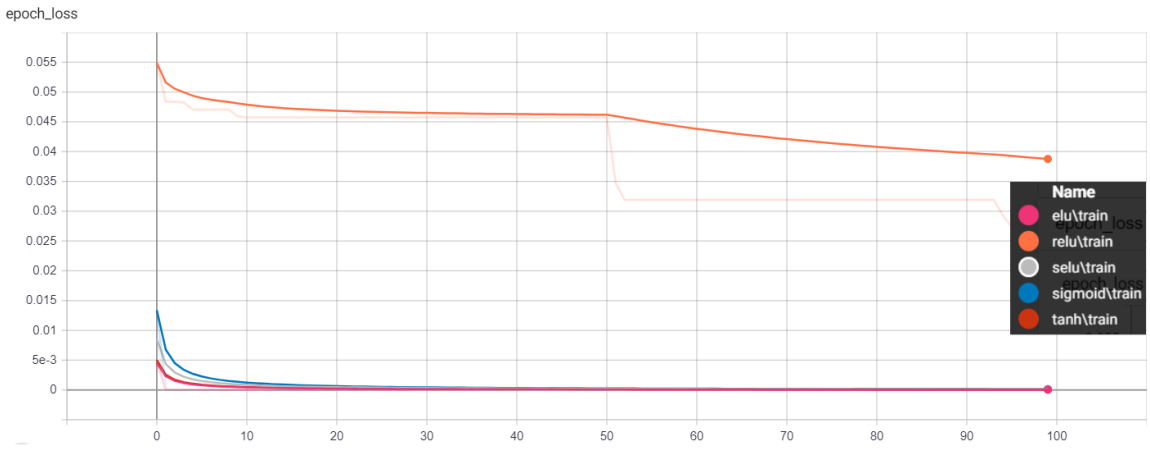


Figure 23: DAE: loss values (5 hidden layers)

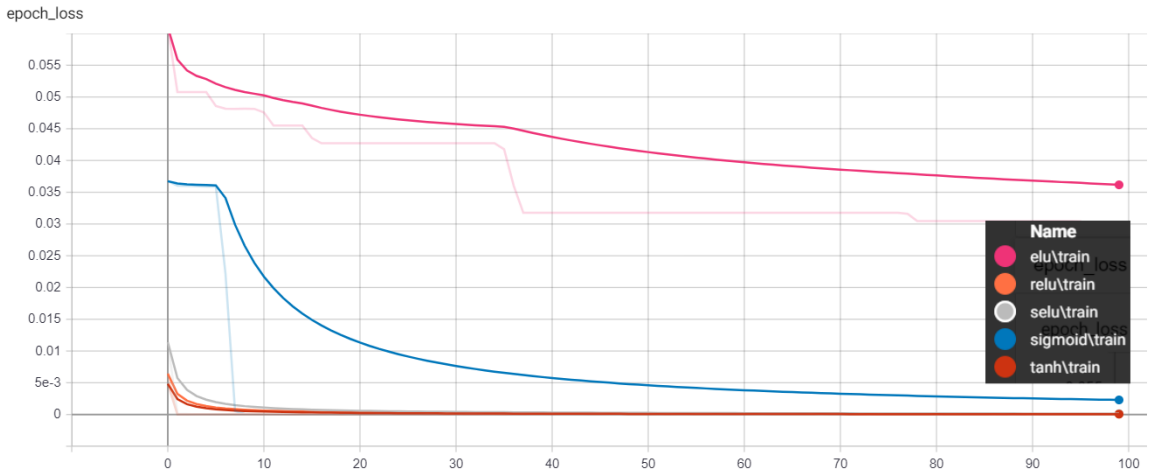


Figure 24: DAE: loss values (9 hidden layers)

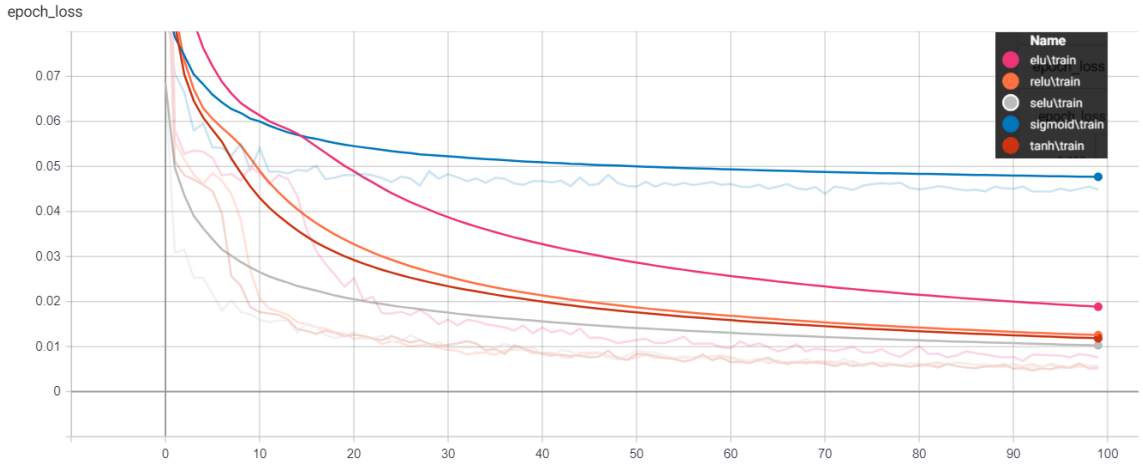


Figure 25: LSTM: loss values (25 units)

5.5 Evaluation Metrics

In order to assess which anomaly detection technique offers better performance, we need to have a set of metrics to evaluate the performance of every technique, whether it is a traditional machine learning or deep learning technique. Generally, the confusion matrix provides one of the best ways to evaluate the detection performance of any model by providing insights on the prevalence of true positives (TP). In our case, TP corresponds to the number of positive alarms, meaning the data that is anomalous and that the detection technique succeeds to detect. True negatives (TN), correspond to the amount of data that

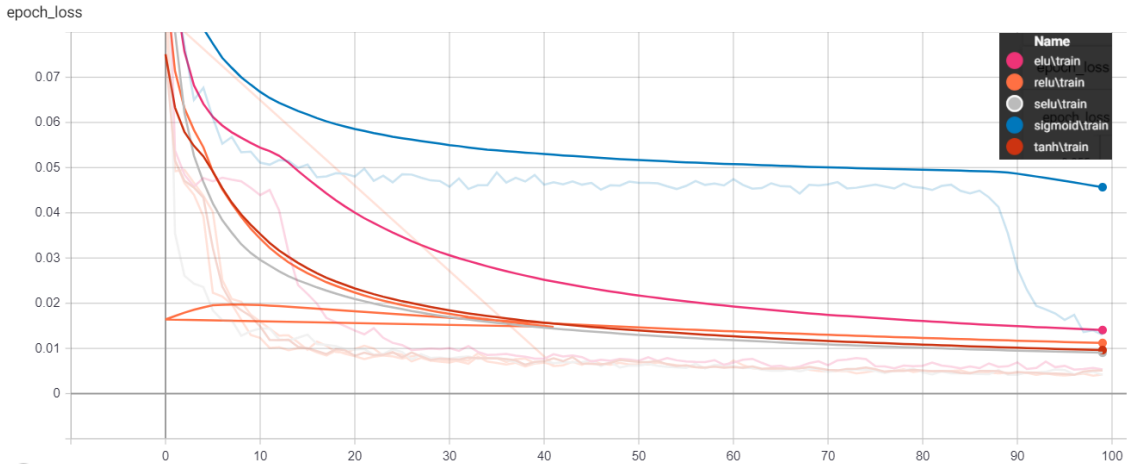


Figure 26: LSTM: loss values (50 units)

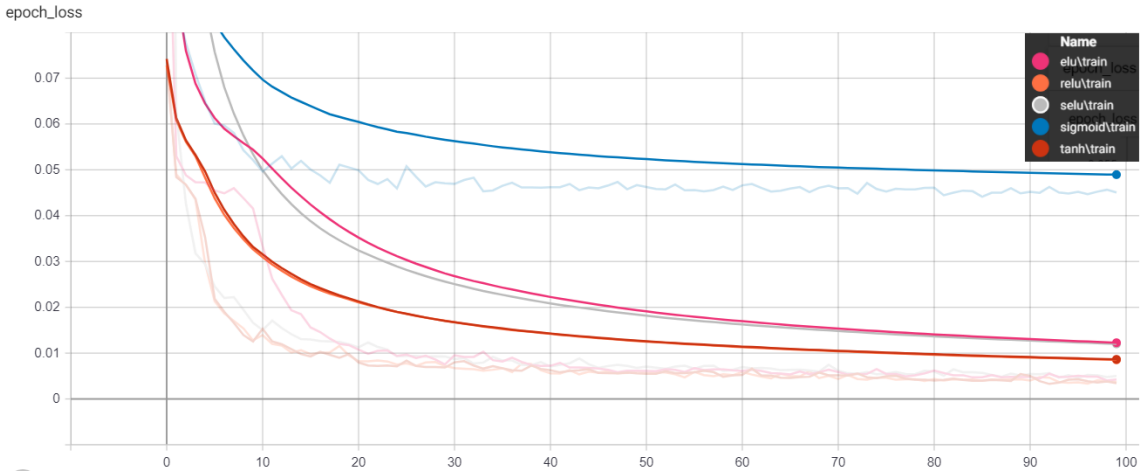


Figure 27: LSTM: loss values (75 units)

is normal, and deemed as normal by the detection technique. In contrast, false positives (FP) and false negatives (FN) occur respectively when a technique deems normal values as anomalous or vice-versa. A detection technique under-performs when it has a high prevalence of false positives (FP) and false negatives (FN). Table 2 shows how a confusion matrix looks like.

As we explain above, a confusion matrix is described as follows:

- TP indicates when an instance is positive and it is predicted as positive.
- TN indicates when an instance is negative and it is predicted as negative.

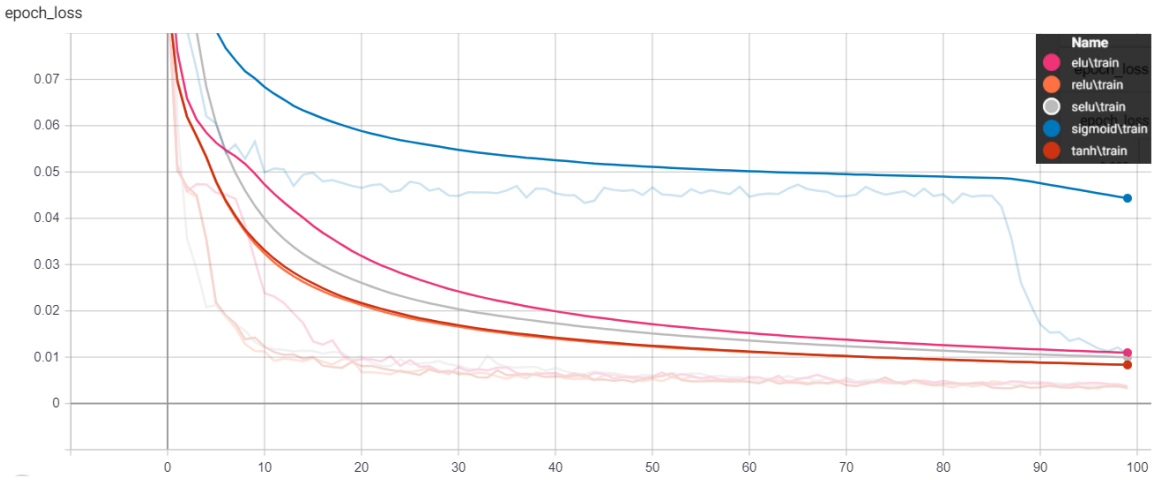


Figure 28: LSTM: loss values (100 units)

Table 2: Confusion Matrix

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

- FP indicates when an instance is negative and it is predicted as positive.
- FN indicates when an instance is positive and it is predicted as negative.

The confusion matrix is not the only way to evaluate the performance of these learning techniques. Other important metrics are the accuracy of the model and the F1 score. We use the accuracy as one of the metrics since it indicates how accurate was the machine learning or deep learning technique in predicting normal and abnormal instances. The metric is mathematically calculated by dividing the number of instances correctly predicted (the sum of TP and TN) over the total number of instances, as per Equation 2.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

As for the F1 score, it requires supplementary values to be calculated. These values are

called the 'precision' and the 'recall'. Precision is about how precise the learning technique is in detecting the instances in given datasets, as per Equation 3. Recall is given by the count of TP instances divided by the actual positives (the sum of TP and FN), as per Equation 4.

$$precision = \frac{TP}{TP + FP} \tag{3}$$

$$recall = \frac{TP}{TP + FN} \tag{4}$$

Using Equation 3 and Equation 4, the F1 score is obtained as per Equation 5.

$$F_1 = \frac{2 \cdot precision \cdot recall}{precision + recall} \tag{5}$$

5.6 Results and Discussion

In this section we provide the details on the performance of the machine learning and deep learning techniques that we are employing. Moreover, we demonstrate how they perform with the distribution automation system under different types of scenarios. Different attacks against specific applications have are exercised in our system, which include: FLISR, Feeder Reconfiguration, and Voltage Control. Also, we try different sets of faults on the system to see their impacts on the data directly. The obtained performance results involve the accuracy, precision, recall, F1 score, as well as the confusion matrix.

Prediction using LSTM. Starting with LSTM, we evaluate the results and compare them by checking the prediction against the real data (whether it was appropriate as it should be or not). While performing hyper parameter tuning, we notice that using different amounts of LSTM units could eventually lead to obtaining better results. We also notice that using *Tanh* activation function would give the best results, while *Elu* is also quite close in terms

of results to *Tanh*. We show in the figures 29, 30, 31, 32, 33, 34, 35, 36, 37, and 38 the results of the predictions for 50 units compared to 100 units, using the different activation functions. We show the results obtained using 50 and 100 units, as these values allow to get the best performance. The performance was not as good for values lower than 50 and plateaued at 100 LSTM units.

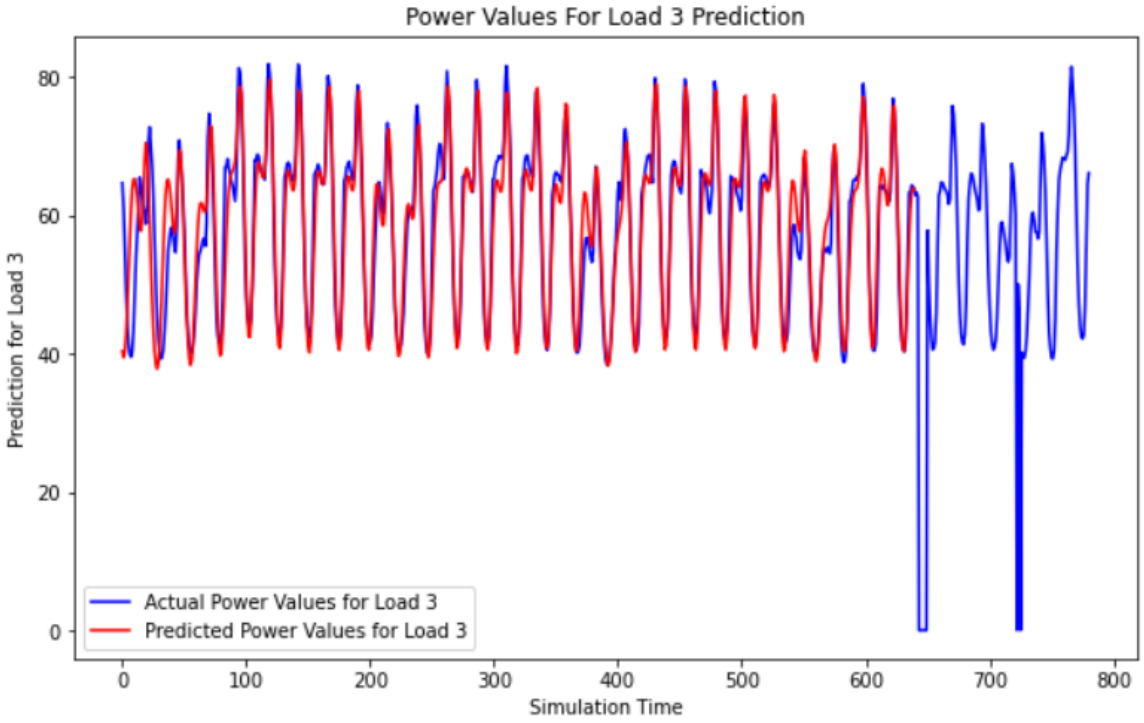


Figure 29: Predicted power values of load 3: 50 units/tanh

Anomaly Detection Techniques Results. Since we basically use LSTM for the prediction of the power values, we can use it for different sets of measurements. The idea of using LSTM is to predict the values from any given fresh datasets (different than the one used for training) and trying to estimate the values appropriately. If the prediction is beyond a certain threshold, an anomaly is flagged. It should be mentioned that the original intention of LSTM as a tool is not for anomaly detection. However, it can be used for anomaly detection purposes. We have the other anomaly detection techniques previously mentioned,

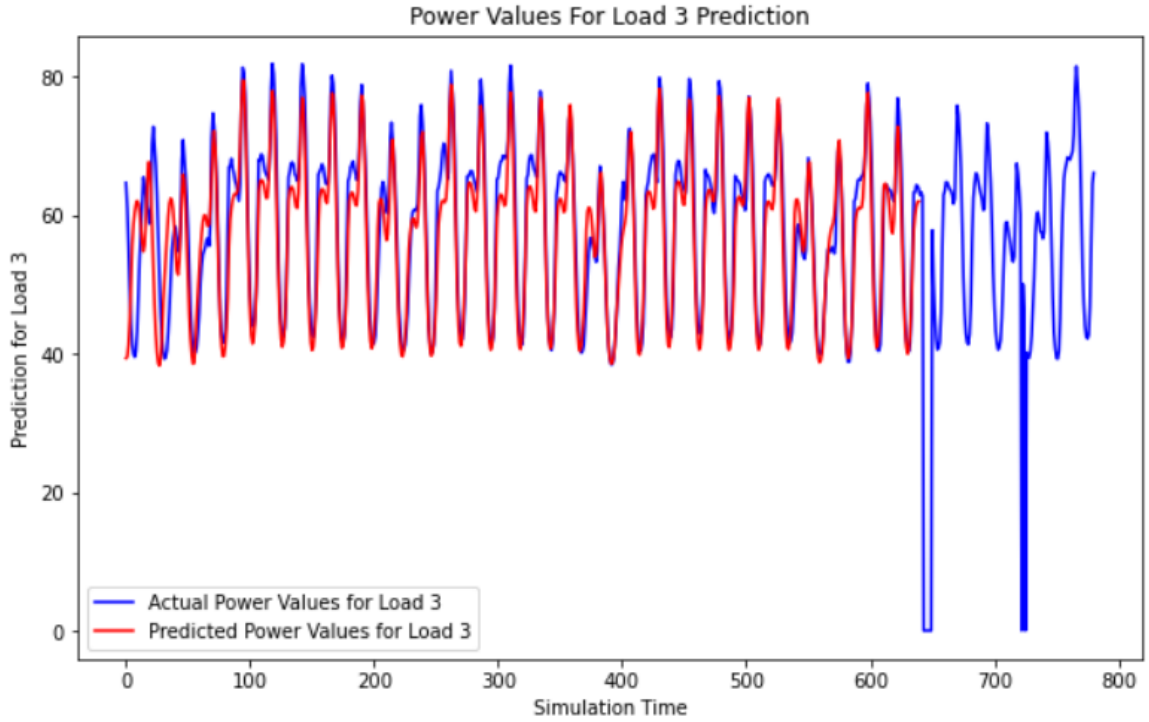


Figure 30: Predicted power values of load 3: 50 units/elu

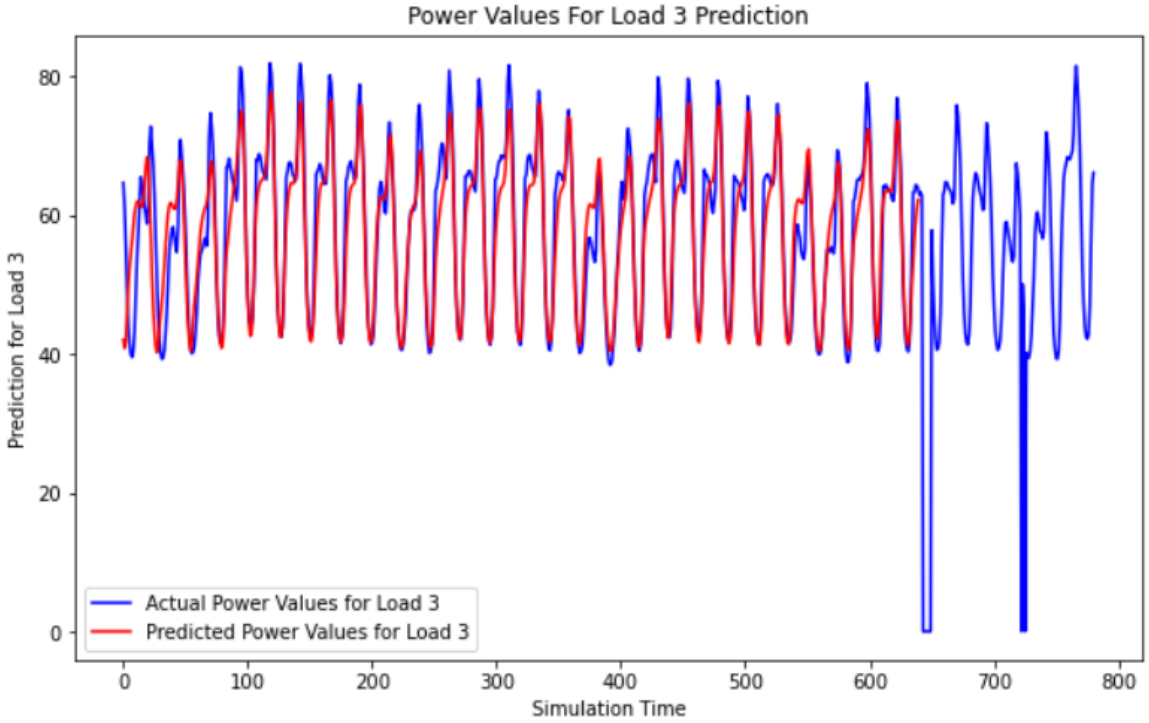


Figure 31: Predicted power values of load 3: 50 units/relu

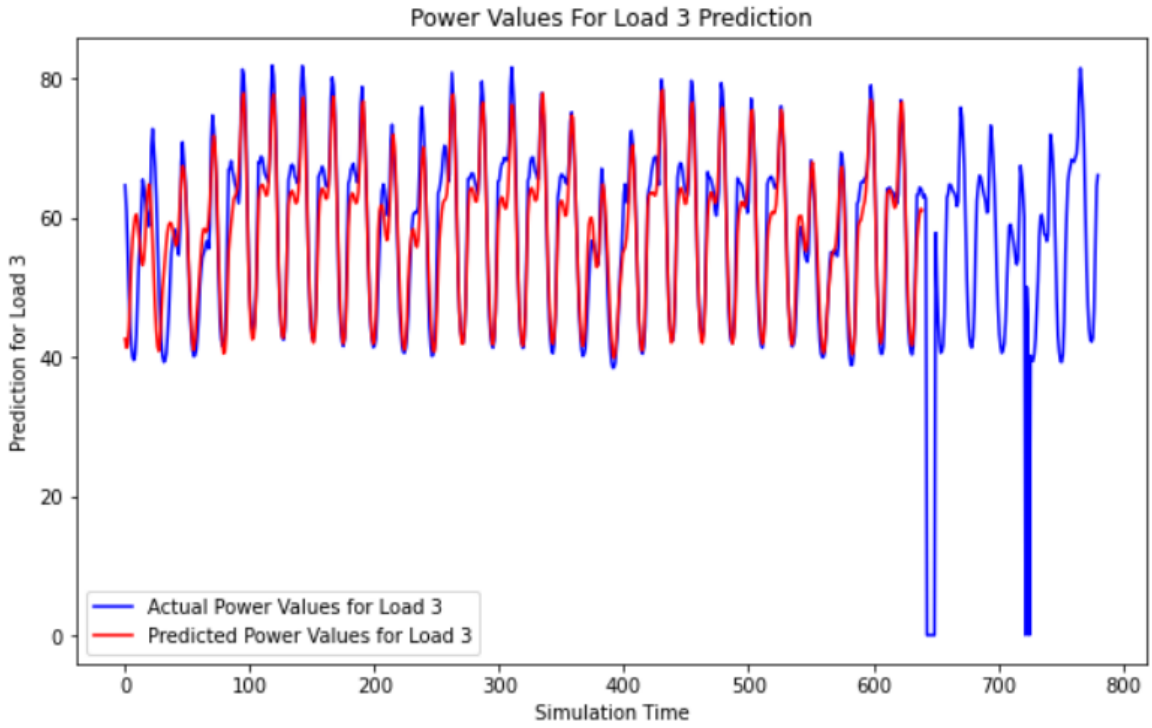


Figure 32: Predicted power values of load 3: 50 units/selu

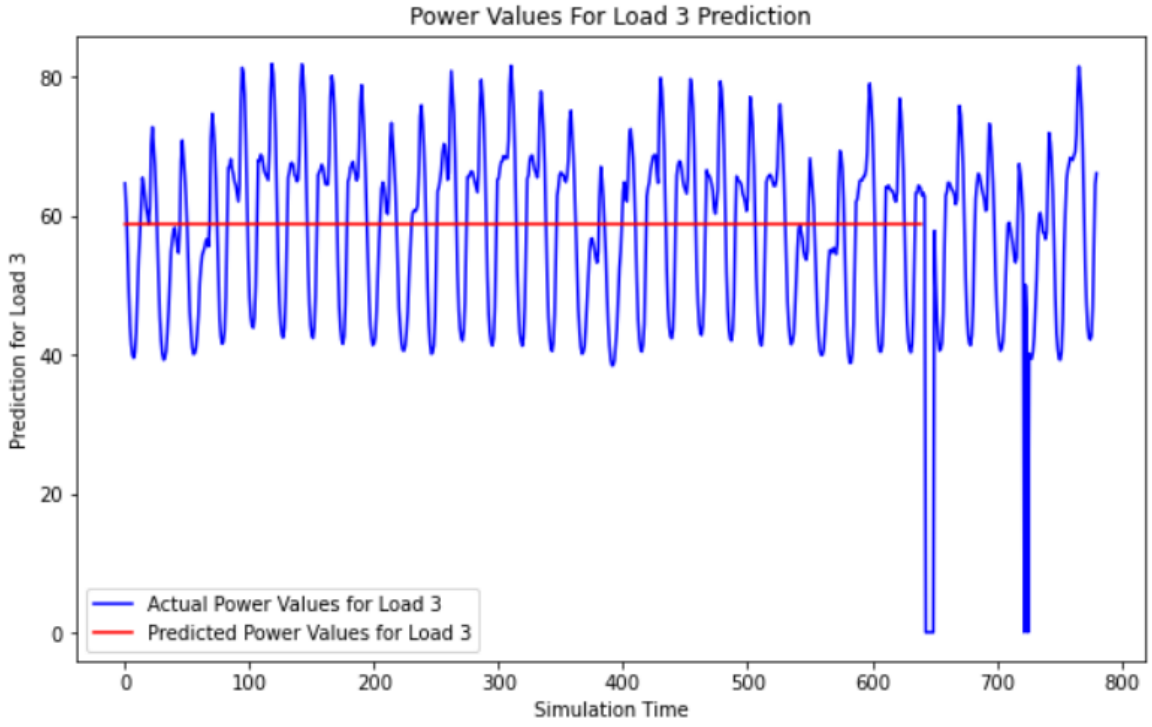


Figure 33: Predicted power values of load 3: 50 units/sigmoid

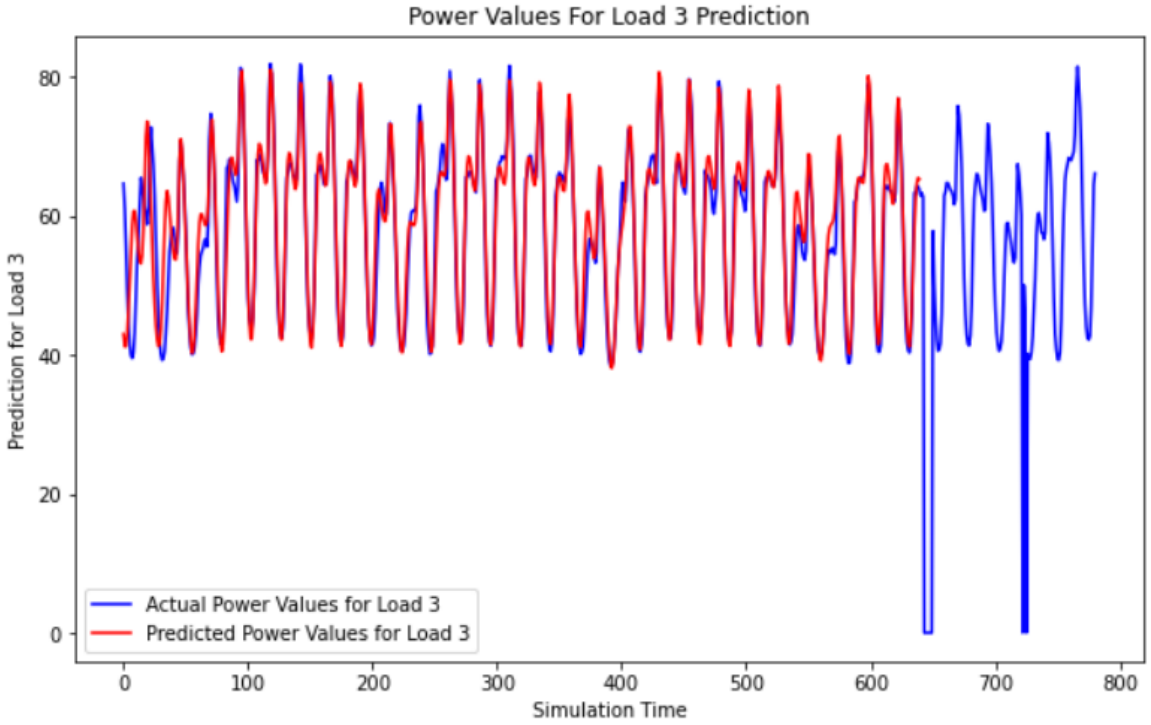


Figure 34: Predicted power values of load 3: 100 units/tanh

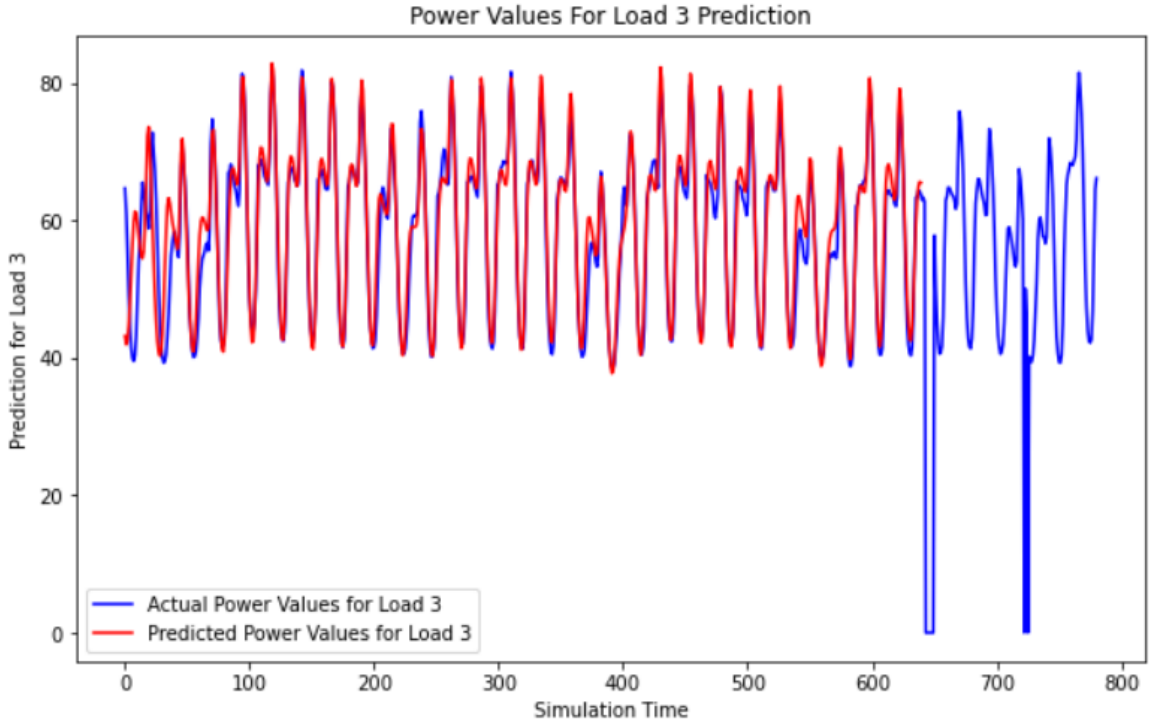


Figure 35: Predicted power values of load 3: 100 units/elu

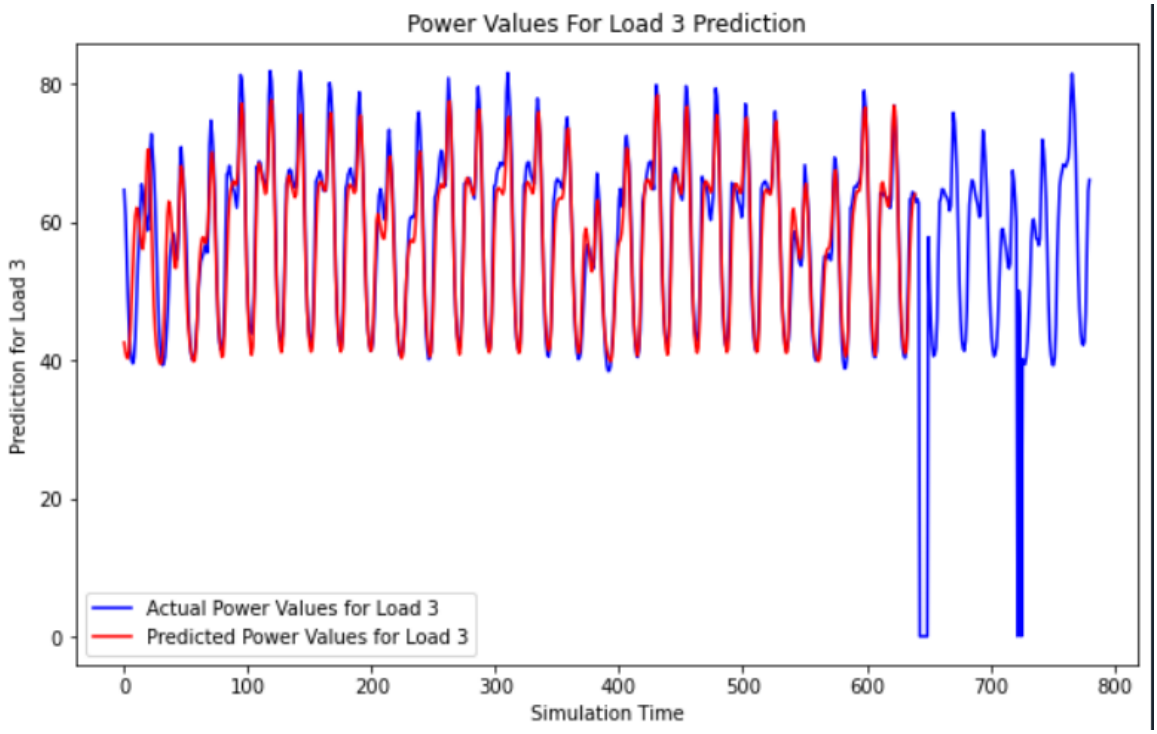


Figure 36: Predicted power values of load 3: 100 units/relu

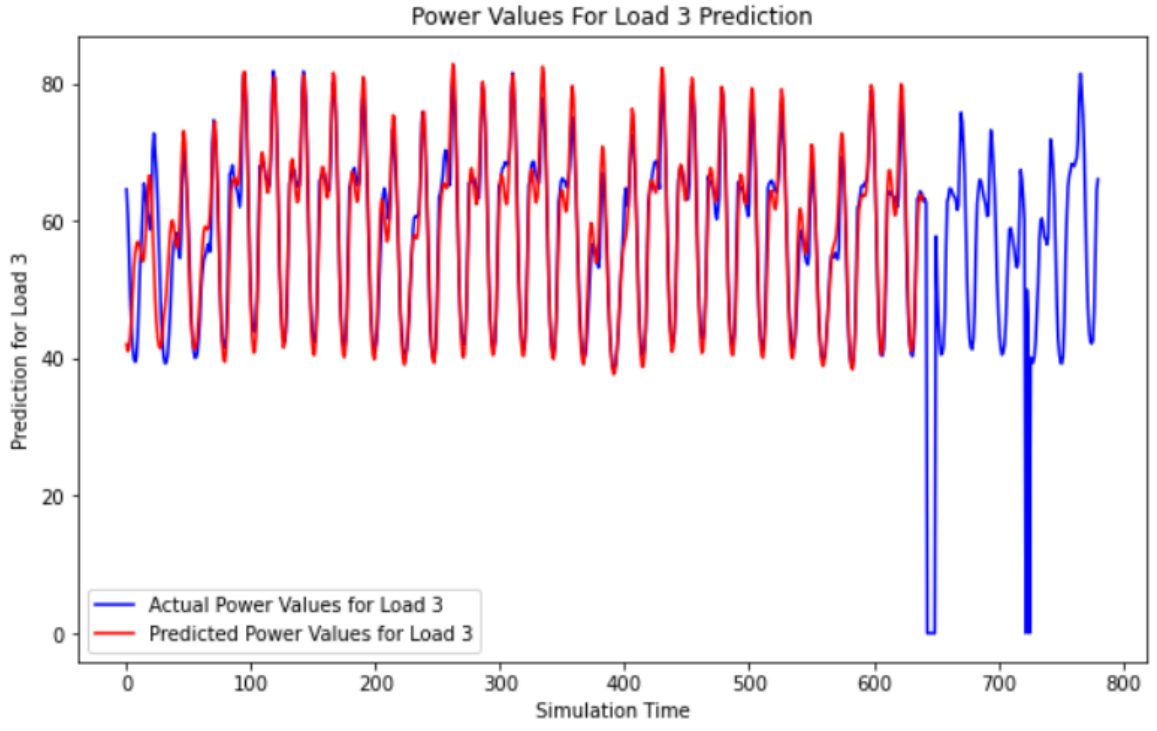


Figure 37: Predicted power values of load 3: 100 units/selu

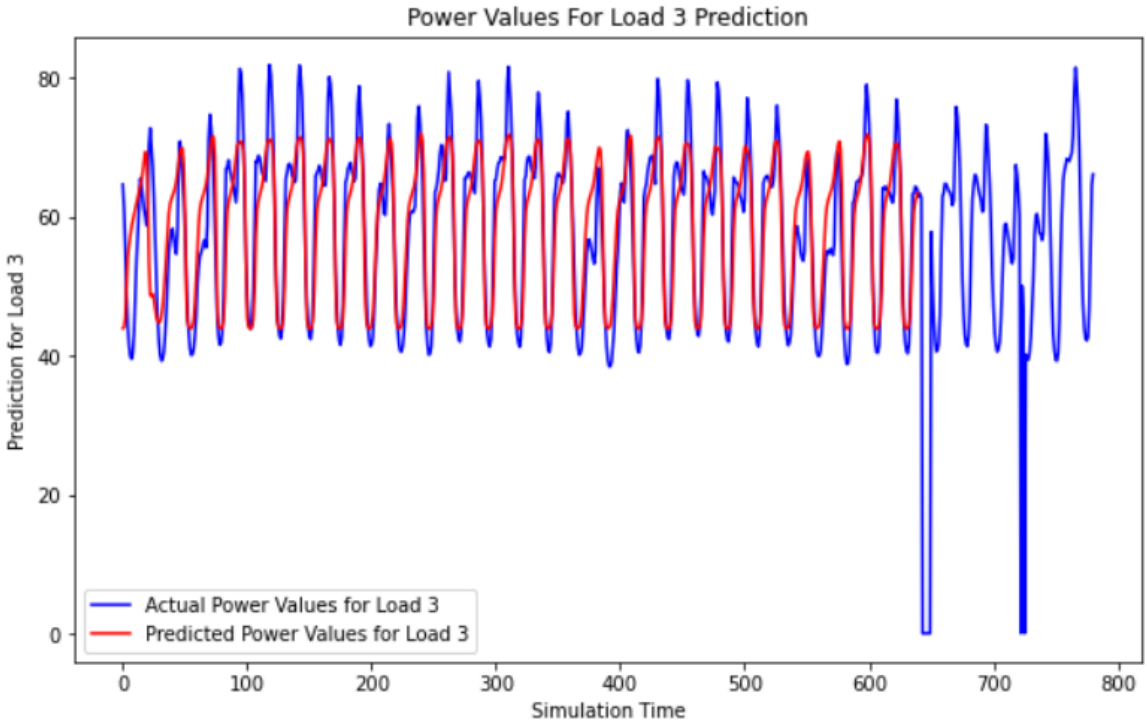


Figure 38: Predicted power values of load 3: 100 units/sigmoid

and in this subsection, we provide the general metrics to compare these techniques against each other and determine which technique is performing better in detecting anomalies in our data. During the data collection, the different scenarios mentioned previously are occurring while the system in running. The idea is to have the different scenarios reflected in the data. The collected data is then fed to different detection techniques. Then, we compare the results among the different techniques in terms of F1 score, recall, precision, accuracy, and the numbers of positive and negative alarms along with the wrongly predicted ones. Table 3 shows the results for the supervised machine learning techniques.

Finally, for the Deep Auto Encoders Technique, the best ways to measure the performance is to use the loss and the reconstruction error values as metrics. However, we can have the accuracy of the model on detecting anomalies on the data while testing. We achieve a 92.26236% accuracy with Deep Auto Encoders. It is safe to mention that machine learning algorithms are faster for detecting anomalies. From Table 3, we notice that

Table 3: Results of Different Supervised Machine Learning Models

	k-NN	**XGBoost**	**DT**	**RF**	**MLP**	**SVM**
TN	28	26	29	29	28	29
FP	1	1	0	0	1	0
FN	0	0	1	0	0	1
TP	1235	1237	1234	1235	1235	1234
Accuracy	0.999208	0.999208	0.999208	1.0	0.999208	0.999208
Recall	0.965517	0.962962	1.0	1.0	0.965517	1.0
Precision	1.0	1.0	0.966666	1.0	1.0	0.966666
F1-Score	0.98245	0.981132	0.9830508	1.0	0.982456	0.9830508

different algorithms achieve over 99.9% accuracy values, with Random Forest technique achieving a 100% accuracy in classifying correctly the data without having false alarms.

Chapter 6

Conclusion

Power distribution systems are an integral part of electrical grids, which are essential for our modern society. The dawn of smart grids, required a corresponding upgrade of traditional power distribution systems as well. This upgrade mandates the integration of fast and reliable communication technologies, and the implementation of automation applications, such as, automatic fault localization, isolation, and service restoration, feeder reconfiguration, and voltage regulation. These applications allow the operator to provide stable power to end consumers with minimal power loss. However, this upgrade opens new attack surfaces and vulnerabilities that could be exploited by able adversaries.

In order to counter these emerging threats, this thesis details the design and implementation of a security monitoring platform able to detect cyber attacks on distribution automation systems. To understand the dynamics of such systems, a realistic co-simulation framework was implemented to mimic actual systems. The framework consists of: (i) a software-based power distribution simulator, (ii) a network communication emulation, and (iii) a software-based distribution system's operator that acts as the main controller. The framework leverages the standard protocol used for such systems, namely the IEC 60870-5-104. Moreover, a test case involving the implementation of the IEEE 33-bus system was

achieved using the power simulator. The IEEE 33-bus system was used as it contains multiple types of loads: industrial, residential, and commercial. The implementation of the test case was comprehensively validated based on the IEEE standard. In order to add the automation aspect of distribution automation systems, the previously mentioned automation application have been implemented within the framework at the level of the distribution system's operator.

The main contribution of this thesis is two-fold. The first one is the implementation of the co-simulation framework. This implementation allows for: a) the collection of realistic telemetry data, and b) the study of the impacts of cyber attacks on distribution automation systems. The second contribution involved, the analysis of the collected telemetry data, which allowed crafting new and elaborated cyber attacks on distribution automation systems that can bypass the bad data detectors that are in place. In addition, new detection techniques have been designed and implemented. Thus, we evaluated the suitability and performance of several machine and deep learning algorithms to design improved detection methods that allow detecting the highly elaborated attacks. We conducted extensive experiments to evaluate multiple techniques. The obtained results indicate that both traditional machine learning and deep learning techniques are suitable to detect anomalies with good accuracy values (greater than 92%). However, Multi Layer Perceptron, Decision Trees, and Random Forest techniques provided the best performance, with an accuracy of 98%.

To the best of our knowledge, the elaborated co-simulation framework is the very first to emulate the IEC 60870-5-104 protocol, which allowed to collect realistic data. Similarly, this research work is the first to use OpenDSS-G as a power simulator with the complete implementation of distribution automation application for the IEEE 33-bus system. The framework is scalable in terms of both communication and power simulation. We exercised the framework to simulate up to the IEEE 123-bus system. Finally, a real-time dashboard

was implemented allowing to monitor different system measurements and to detect anomalies. The framework also provides the ability to simulate the execution of various attacks in order to observe the impacts on the distribution automation system.

The framework could be further improved by implementing other communication protocols typically used, such as DNP3 and MODBUS. Also, designing and implementing additional distribution automation applications could be useful for the distribution system's operator. For the security monitoring side, analysing the suitability of other detection techniques such as, Generative Adversarial Networks, and deploying them accordingly could enhance the detection capability.

Bibliography

[1] The smart grid could hold the keys to electric vehicles by chris nicholson. https://innovationatwork.ieee.org/the-smart-grid-could-hold-the-keys-to-electric-vehicles/.

[2] Souhila Aoufi, Abdelouahid Derhab, and Mohamed Guerroumi. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *Journal of Information Security and Applications*, 54:102518, 2020.

[3] Aized Amin Soofi and Arshad Awan. Classification techniques in machine learning: applications and issues. *Journal of Basic and Applied Sciences*, 13:459–465, 2017.

[4] U.s. departement of energy smart grid system report 2018. https://www.energy.gov/sites/prod/files/2019/02/f59/Smart%20Grid%20System%20Report%20November%202018_1.pdf. Accessed on: 2020/14/12.

[5] Smart grid in canada. https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/canmetenergy/pdf/Smart%20Grid%20in%20Canada%20Report%20Web%20FINAL%20EN.pdf. Accessed on: 2020/14/12.

[6] Nova scotia power set to roll out smart meters following uarb approval. https://www.nspower.ca/smartmeters. Accessed on: 2020/14/12.

[7] Cyber threat and vulnerability analysis of the u.s. electric sector. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf. Accessed on: 2020/14/12.

[8] Blackenergy by the sshbeardoor: attacks against ukrainian news media and electric industry by anton cherepanov. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/. Accessed on: 2021-01-01.

[9] Win32/industroyer a new threat for industrial control systems by anton cherepanov, eset. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf. Accessed on: 2021-01-01.

[10] M. A. M, A. M. Atallah, A. Abdel-Sattar, and M. A. El-Dessouki. Various communication technologies used in smart grid. In *2019 21st International Middle East Power Systems Conference (MEPCON)*, pages 1101–1106, 2019.

[11] Thomas Allen Short. *Electric power distribution handbook*. CRC press, 2014.

[12] Abdelhay A Sallam and Om P Malik. *Electric distribution systems*. John Wiley & Sons, 2018.

[13] Daniel E Nordell. Communication systems for distribution automation. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, pages 1–14. IEEE, 2008.

[14] Yazhou Jiang, Chen-Ching Liu, and Yin Xu. Smart distribution systems. *Energies*, 9(4):297, 2016.

[15] Daniel A Haughton and Gerald Thomas Heydt. A linear state estimation formulation for smart distribution systems. *IEEE Transactions on Power Systems*, 28(2):1187–1195, 2012.

[16] Jianzhong Wu, Yan He, and Nick Jenkins. A robust state estimator for medium voltage distribution networks. *IEEE Transactions on Power Systems*, 28(2):1008–1016, 2012.

[17] Sang-Yun Yun, Pyeong-Ik Hwang, Seung-Il Moon, Seong-Chul Kwon, Il-Keun Song, and Joon-Ho Choi. Development and field test of voltage var optimization in the korean smart distribution management system. *Energies*, 7(2):643–669, 2014.

[18] Marko Kolenc, Igor Papič, and Boštjan Blažič. Minimization of losses in smart grids using coordinated voltage control. *Energies*, 5(10):3768–3787, 2012.

[19] Juan Li, Xi-Yuan Ma, Chen-Ching Liu, and Kevin P Schneider. Distribution system restoration with microgrids using spanning tree search. *IEEE Transactions on Power Systems*, 29(6):3021–3029, 2014.

[20] Mohammad Heidari Kapourchali, Mojtaba Sepehry, and Visvakumar Aravinthan. Fault detector and switch placement in cyber-enabled power distribution network. *IEEE Transactions on Smart Grid*, 9(2):980–992, 2016.

[21] U.s. department of energy. smart grid investment grant program. progress report. `https://www.energy.gov/oe/downloads/smart-grid-investment-grant-program-progress-report-october-2013`. Accessed on: 2019-12-08.

[22] Mohiuddin Ahmed and Al-Sakib Khan Pathan. False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, 8:1–14, 2020.

[23] TE McDermott, RC Dugan, TL King, and MF McGranaghan. Modelling distribution automation schemes with a control systems overlay. In *2009 IEEE Power & Energy Society General Meeting*, pages 1–3. IEEE, 2009.

[24] Michele Garau, Emilio Ghiani, Gianni Celli, Fabrizio Pilo, and Sergio Corti. Co-simulation of smart distribution network fault management and reconfiguration with lte communication. *Energies*, 11(6):1332, 2018.

[25] MR Elkadeem, MA Alaam, and Ahmed M Azmy. Improving performance of underground mv distribution networks using distribution automation system: A case study. *Ain Shams Engineering Journal*, 9(4):469–481, 2018.

[26] D Bian, M Kuzlu, M Pipattanasomporn, S Rahman, and Yiming Wu. Real-time co-simulation platform using opal-rt and opnet for analyzing smart grid performance. In *2015 IEEE Power & Energy Society General Meeting*, pages 1–5. IEEE, 2015.

[27] Shilei Guan, Wenbo Fan, Haoliang Lei, Lan Liu, and Dongliang Li. Realization of a simulation test method for feeder automation of power distribution automation system. In *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, pages 2710–2714. IEEE, 2015.

[28] D Montenegro, M Hernandez, and GA Ramos. Real time opendss framework for distribution systems simulation and analysis. In *2012 Sixth IEEE/PES Transmission and Distribution: Latin America Conference and Exposition (T&D-LA)*, pages 1–5. IEEE, 2012.

[29] Bok-Nam Ha, SW Lee, CH Shin, SC Kwon, SY Park, and MH Park. Development of intelligent distribution automation system. In *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific*, pages 1–4. IEEE, 2009.

[30] Carol Hawk and Akhlesh Kaushiva. Cybersecurity and the smarter grid. *The Electricity Journal*, 27(8):84–95, 2014.

[31] Arif Wazir and Naeem Arbab. Analysis and optimization of ieee 33 bus radial distributed system using optimization algorithm. *Journal of Emerging Trends in Applied Engineering*, 1(2):17–21, 2016.

[32] Timothy R Vittor, T Sukumara, SD Sudarsan, and Janne Starck. Cyber security-security strategy for distribution management system and security architecture considerations. In *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pages 1–6. IEEE, 2017.

[33] Jean-Luc Batard, Yves Chollot, Patrick Pipet, Ludovic Lamberti, and Adam Gauci. Cybersecurity for modern distribution automation grids. *CIRED-Open Access Proceedings Journal*, 2017(1):1002–1005, 2017.

[34] IH Lim, S Hong, Myeon-Song Choi, Seung-Jae Lee, SW Lee, and BN Ha. Applying security algorithms against cyber attacks in the distribution automation system. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, pages 1–6. IEEE, 2008.

[35] Ishtiaq Ahmad, Jawad Haider Kazmi, Mohsin Shahzad, Peter Palensky, and Wolfgang Gawlik. Co-simulation framework based on power system, ai and communication tools for evaluating smart grid applications. In *2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA)*, pages 1–6. IEEE, 2015.

[36] Jacques Benoit, Serge Gagnon, Luc Tétreault, and Automation Engineer. Securing distribution automation. In *Western Power Delivery Automation Conference*, 2010.

[37] DMDK Dissanayaka, KTMU Hemapala, and WDAS Rodrigo. Fault management algorithm for voltage feeder automation in electricity distribution. *Annual Sessions of IESL*, pages 119–126, 2016.

[38] Liang Hu, Zidong Wang, Qing-Long Han, and Xiaohui Liu. State estimation under false data injection attacks: Security analysis and system protection. *Automatica*, 87:176–183, 2018.

[39] JS Savier and Debapriya Das. Impact of network reconfiguration on loss allocation of radial distribution systems. *IEEE Transactions on Power Delivery*, 22(4):2473–2480, 2007.

[40] M Zekeriya Gunduz and Resul Das. Analysis of cyber-attacks on smart grid applications. In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pages 1–5. IEEE, 2018.

[41] Xiaming Ye, Junhua Zhao, Yan Zhang, and Fushuan Wen. Quantitative vulnerability assessment of cyber security for distribution automation systems. *Energies*, 8(6):5266–5286, 2015.

[42] Rong Fu, Xiaojuan Huang, Yusheng Xue, Yingjun Wu, Yi Tang, and Dong Yue. Security assessment for cyber physical distribution power system under intrusion attacks. *IEEE Access*, 7:75615–75628, 2018.

[43] IH Lim, S Hong, MS Choi, SJ Lee, TW Kim, SW Lee, and BN Ha. Security protocols against cyber attacks in the distribution automation system. *IEEE Transactions on Power Delivery*, 25(1):448–455, 2009.

[44] Radosław Rekowski, Krzysztof Dobrzyński, and Zbigniew Lubośny. The impact of the distribution network reconfiguration on active power losses: Selected issues of upgrid project realization. In *2017 IEEE 21st International Conference on Intelligent Engineering Systems (INES)*, pages 000247–000252. IEEE, 2017.

[45] Lindah Kotut and Luay A Wahsheh. Survey of cyber security challenges and solutions in smart grids. In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 32–37. IEEE, 2016.

[46] Abdelrahman Ayad, Hany Farag, Amr Youssef, and Ehab El-Saadany. Cyber–physical attacks on power distribution systems. *IET Cyber-Physical Systems: Theory & Applications*, 2020.

[47] Yasunori Isozaki, Shinya Yoshizawa, Yu Fujimoto, Hideaki Ishii, Isao Ono, Takashi Onoda, and Yasuhiro Hayashi. Detection of cyber attacks against voltage control in distribution power grids with pvs. *IEEE Transactions on Smart Grid*, 7(4):1824–1835, 2015.

[48] Amr E Mohamed. Comparative study of four supervised machine learning techniques for classification. *International Journal of Applied*, 7(2), 2017.

[49] FY Osisanwo, JET Akinsola, O Awodele, JO Hinmikaiye, O Olakanmi, and J Akinjobi. Supervised machine learning algorithms: classification and comparison. *International Journal of Computer Trends and Technology (IJCTT)*, 48(3):128–138, 2017.

[50] Jacob Sakhnini, Hadis Karimipour, and Ali Dehghantanha. Smart grid cyber attacks detection using supervised learning and heuristic feature selection. In *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pages 108–112. IEEE, 2019.

[51] 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.

[52] Michael D Twa, Srinivasan Parthasarathy, Cynthia Roberts, Ashraf M Mahmoud, Thomas W Raasch, and Mark A Bullimore. Automated decision tree classification of corneal shape. *Optometry and vision science: official publication of the American Academy of Optometry*, 82(12):1038, 2005.

[53] Carla E Brodley and Paul E Utgoff. *Multivariate versus univariate decision trees*. University of Massachusetts, Department of Computer and Information Science ..., 1992.

[54] J. Ross Quinlan. Induction of decision trees. *Machine learning*, 1(1):81–106, 1986.

[55] Devi Prasad Bhukya and S Ramachandram. Decision tree induction: an approach for data classification using avl-tree. *International Journal of Computer and Electrical Engineering*, 2(4):660, 2010.

[56] Ying Yang and Geoffrey I Webb. Discretization for naive-bayes learning: managing discretization bias and variance. *Machine learning*, 74(1):39–74, 2009.

[57] Nir Friedman, Moises Goldszmidt, et al. Discretizing continuous attributes while learning bayesian networks. In *ICML*, pages 157–165, 1996.

[58] Shuang-cheng Wang, Rui Gao, and Li-min Wang. Bayesian network classifiers based on gaussian kernel density. *Expert Systems with Applications*, 51:207–217, 2016.

[59] P Myllymaki. Advantages of bayesian networks in data mining and knowledge discovery, 2010.

[60] Thomas Cover and Peter Hart. Nearest neighbor pattern classification. *IEEE transactions on information theory*, 13(1):21–27, 1967.

[61] Hui Li, Ling Liu, Xiao Zhang, and Shan Wang. Hike: A high performance knn query processing system for multimedia data. In *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, pages 296–303. IEEE, 2015.

[62] Putu Wira Buana, SDRM Jannet, IKGD Putra, et al. Combination of k-nearest neighbor and k-means based on term re-weighting for classify indonesian news. *International Journal of Computer Applications*, 50(11):37–42, 2012.

[63] Nitin Bhatia et al. Survey of nearest neighbor techniques. *arXiv preprint arXiv:1007.0085*, 2010.

[64] Xindong Wu, Vipin Kumar, J Ross Quinlan, Joydeep Ghosh, Qiang Yang, Hiroshi Motoda, Geoffrey J McLachlan, Angus Ng, Bing Liu, S Yu Philip, et al. Top 10 algorithms in data mining. *Knowledge and information systems*, 14(1):1–37, 2008.

[65] Vladimir Vapnik. *The nature of statistical learning theory*. Springer science & business media, 2013.

[66] AH Nizar, ZY Dong, and Y Wang. Power utility nontechnical loss analysis with extreme learning machine method. *IEEE Transactions on Power Systems*, 23(3):946–955, 2008.

[67] Iftikhar Ahmad, Azween B Abdulah, and Abdullah S Alghamdi. Towards the designing of a robust intrusion detection system through an optimized advancement of neural networks. In *Advances in Computer Science and Information Technology*, pages 597–602. Springer, 2010.

[68] Svm by nick gillian. `http://www.nickgillian.com/wiki/pmwiki.php/GRT/SVM`.

[69] Lijuan Cao and Francis EH Tay. Financial forecasting using support vector machines. *Neural Computing & Applications*, 10(2):184–192, 2001.

[70] Md Zahangir Alom and Tarek M Taha. Network intrusion detection for cyber security using unsupervised deep learning approaches. In *2017 IEEE National Aerospace and Electronics Conference (NAECON)*, pages 63–69. IEEE, 2017.

[71] Pascal Vincent, Hugo Larochelle, Isabelle Lajoie, Yoshua Bengio, Pierre-Antoine Manzagol, and Léon Bottou. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. *Journal of machine learning research*, 11(12), 2010.

[72] Zachary C Lipton, John Berkowitz, and Charles Elkan. A critical review of recurrent neural networks for sequence learning. *arXiv preprint arXiv:1506.00019*, 2015.

[73] L Busk Linnebjerg and R Wetke. Long short term memory. *Hear. Balanc. Commun.*, 12:36–40, 1997.

[74] Junyoung Chung, Caglar Gulcehre, KyungHyun Cho, and Yoshua Bengio. Empirical evaluation of gated recurrent neural networks on sequence modeling. *arXiv preprint arXiv:1412.3555*, 2014.

[75] Yoshua Bengio. *Learning deep architectures for AI*. Now Publishers Inc, 2009.

[76] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

[77] Arwa Aldweesh, Abdelouahid Derhab, and Ahmed Z Emam. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189:105124, 2020.

[78] Lstm made simple. `https://medium.com/mlreview/understanding-lstm-and-its-diagrams-37e2f46f1714`. Accessed on: 2020-08-20.

[79] Ali Abur and Antonio Gomez Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004.

[80] A Monticelli. Fast decoupled state estimator. In *State Estimation in Electric Power Systems*, pages 313–342. Springer, 1999.