REPUBLIC OF TÜRKIYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

WIRELESS LAN DESIGN AND FUTURE INTERNET ARCHITECTURE

Ashraf Thaker Mahmood ALMUKHTAR

Master's Thesis

Supervisor

Prof. Dr. Osman Nuri UÇAN

Istanbul, 2023

WIRELESS LAN DESIGN AND FUTURE INTERNET ARCHITECTURE

Ashraf Thaker Mahmood ALMUKHTAR

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled WIRELESS LAN DESIGN AND FUTURE INTERNET ARCHITECTURE prepared by Ashraf Thaker Mahmood ALMUKHTAR and submitted on 04/04/2023 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

_____

Prof. Dr. Osman Nuri UÇAN

Supervisor

Thesis Defense instead of Jury Members:

Prof. Dr. Osman Nuri UÇAN	Faculty Of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Sefer KURNAZ	Faculty Of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Adil Deniz DURU	Faculty of Physical Education and Sports, Marmara University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master thesis Submission date of the thesis to the Graduate Education Institute: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Ashraf Thaker Mahmood ALMUKHTAR

Signature

DEDICATION

I dedicate and promise this study to my supervisor Prof. Dr. Osman Nuri UÇAN, who was instrumental in helping me through the entire research process, as well as my family (my father is the role model, my beloved mother, my dear wife, my beloved children) and my beloved brother and sisters, who have always been my support during difficult times.

PREFACE

First and foremost, I want to express my gratitude to my supervisor, Prof. Dr. Osman Nuri UÇAN, for guiding and assisting me during the composition of this dissertation. Every week, I met with my supervisor, Prof. Dr. Osman Nuri UÇAN, to discuss my progress, challenges, and suggestions. This helped me enormously in grasping the reasoning behind the research. It helped me understand the technological requirements for this study project.

ABSTRACT

WIRELESS LAN DESIGN AND FUTURE INTERNET ARCHITECTURE

ALMUKHTAR, Ashraf Thaker Mahmood

M.Sc., Electrical and Computer Engineering, Altınbaş University

Supervisor: Prof. Dr. Osman Nuri UÇAN

Date: April / 2023

Pages: 60

In this research thesis, Intrusion detection is evolving in WLAN design and future internet architecture. Internationally, individuals are increasingly tech-dependent. Various sectors have coined the term "Internet of Things" (IoT) to capture this trend of using Internet and cloud-based services for administrative and operational tasks like data storage, administration, and monitoring. These assumptions were based on the difficulty of collecting important data from a working WLAN or mission-critical corporate network. WLAN design and future internet architecture are important areas of research in networking, and their implementation on MATLAB can provide valuable insights. MATLAB can be used to model and simulate WLANs and future internet architectures, allowing researchers to evaluate the performance of different design choices and protocols under various conditions. Furthermore, MATLAB can be used to develop and test new algorithms and protocols for WLANs and future internet architectures. This can lead to the development of more efficient and secure networks that can meet the increasing demands of the digital age. Therefore, the use of MATLAB in WLAN design and future internet architecture implementation can greatly contribute to the advancement of networking technology. Sanitized telemetry from a real system would increase simulation accuracy. The signal dynamics could be simulated more correctly. The test could imitate WLAN system activities without real data. The test bed servers may build and operate a small flow loop with sensors and controls. The primary test bed server allows sensor polling, controlling, and data collection (which also acts as the WLAN server). Time-synchronous averaging algorithms resample data from several

telemetry sources with different sampling rates. The freshly developed WLAN variable grouping technique is demonstrated in several case scenarios. Variable grouping methods allow the extraction of model subsets with the lowest prediction errors. The study also examines AAKR and AAMSET results for a sample of successfully detected intrusion actions from two data sets. The models found which Linux kernel telemetry cluster was best for intrusion detection using four clusters. The knowledge-based system is the most extensively used method that detects wireless network assaults using their signatures. This system is easy to set up and has a low false/missed alarm rate, however it cannot detect wireless network zero-day attacks. Zero-day wireless network attacks are undetected. The knowledge-based system will consider the unusual behavior normal because it has never seen a zero-day intrusion incident. The behavior-based technique detects known and unknown wireless network assaults at 97.86%. This modeler analyzes data to predict system behavior. Future intrusions will be telemetry data that does not match the learned behavior.
Keywords: Wireless, Communication, Identification, Classification, Attacks.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

CPS	:	Cyber-Physical Systems
I&C	:	Instrumentation And Control
IDS	:	Intrusion Detection System
FAP	:	False Alarm Probability
NN		Neural Networks
GA	:	Genetic Algorithms
VGM	:	Variable Grouping Methods
AAKR	:	Auto Associative Kernel Regression
MSET	:	Multivariate State Estimation Technique
ACF	:	Auto Correlation Function
SPRT	:	Sequential Probability Ratio Test
SQL		Structure Query Language
HIDS	:	Host Intrusion Detection System
NIDS	:	Network Intrusion Detection System
WLAN		Wireless Local Area Network
MAP		Mapping

1. INTRODUCTION

Cyber-Physical Systems (CPS) have gained popularity in the process control industry as a result of computing's recent breakthroughs. The CPS is a vast, globally distributed system composed primarily of physical components such as industrial equipment, sensors, and actuators. A "cyber component" employs operators and/or servers at a distant control center to monitor, transfer data, or issue commands utilizing a set of specialized communication protocols. Combining sensing and control technology has helped numerous sectors, including the nuclear, petroleum, hydropower, automotive, and railroad industries. These systems are utilized for automated jobs or in inconveniently positioned machinery. The Supervisory Control and Data Acquisition (WLAN) system monitors and manages equipment and operations using data sensing, acquisition, and specialized communications protocols. WLAN systems regulate the distribution of numerous vital resources, such as energy and water, and many industries have recently shifted to a digital Instrumentation and Control (I&C) culture, necessitating the protection of the integrity and security of these systems from malicious, unauthorized, and even authorized users. In the worst-case scenario, damage or suspension of access to these systems could result in power outages for consumers, crop irrigation problems, identity theft, or even fatalities if the WLAN system is responsible for passenger transportation. Stuxnet-scale assaults on WLAN networks are, thankfully, extremely uncommon. But, a few of high-profile incidents from the recent past are sufficient to highlight the aforementioned losses. In 2003, the wireless network of the Slammer worm attempted to enter the Davis-Bessie nuclear power plant [1]. Many monitoring stations were inaccessible for a number of hours due to this wireless network attack. Nobody was in immediate danger, as the plant was not operational and safety precautions were in place. In 2007, an engineer compromised a wireless local area network (WLAN) that controlled the distribution of Sacramento River water for agricultural and home purposes[2].

Again, this disturbance led to a decline in business, and the engineer was severely penalized. In Germany, a collision between two passenger trains finally resulted in injuries and fatalities in 2016 [3]. It was established that the primary plant operator was the principal cause of the tragedy. Despite the fact that two trains were running in opposite directions on the same track, the conductors were given incorrect inputs, and the system alerts were disregarded. It

is evident from this example that not all WLAN security concerns originate from the outside. Next, we'll examine these and additional WLAN network security events in further detail. Considering these instances, it is evident that as more industries transition to digital I&C, the sophistication and quantity of threats to these systems will increase. The prospect of misuse, such as attempting to access sensitive data, manipulate system resources, or open shutdown valves, poses a risk to the security of these systems [4]. These types of security threats can be described using phrases such as zero-day, temporary, and permanent. Using zero-day flaws, attacks on wireless networks are wholly novel and can circumvent many popular security mechanisms. In addition, they often move quickly and engage in temporary attacks on wireless networks. Long-term attacks can cause damage over a longer period of time by inserting malware that masquerades the attacker as an authorized user in order to steal sensitive data or interfere with system functioning. Most of these threats cannot be identified without a detection system. Any hardware and/or software configuration that monitors system telemetry and statuses in search of suspicious behavior might constitute an intrusion detection system (IDS). The IDS may scan wireless network telemetry or records for anomalies or departures from the norm, as well as indications of known intrusion attempts.

These systems may be passive, in which case an alert is sent when a rule is violated, or reactive, in which case action is done to destroy the intruder and/or isolate the problematic system. WLAN system security concerns have prompted the creation of numerous IDS types in the literature. Techniques for identifying intrusions in audit or telemetry data fall into one of several key intrusion detection system groups (IDS). There are three primary classifications of detecting systems: knowledge-based, behavior-based, and behavior-specification-based [5]. The strategy only searches for specific signatures in knowledge-based systems that match to previously neutralized attacks on wireless networks. These signatures are recorded in a document known as an attack dictionary for wireless networks. This has advantages and disadvantages [6], since any signatures not in the lexicon are regarded as normal. One of its virtues is that it is simple to install and creates few false alarms. The strategy's major flaw is its inability to discover brand-new vulnerabilities in wireless networks.

In behavior-based systems, models are trained on data resembling typical operating

conditions, and any deviations from this learned behavior are deemed abnormal [7]. This type often produces a greater proportion of false alarms, necessitates operational data and training time, and has a greater system overhead than knowledge-based systems. In the concluding parts of this thesis, the sequential probability ratio test is used to this topic. Despite these apparent drawbacks, behavior-based IDS offer a significant security advantage over knowledge-based systems by detecting zero-day wireless network attacks. In addition, there is no requirement for enumerating all potential models with this approach. The formal behaviors and specifications of behavior-specification-based systems [8] are pre-programmed by a human specialist. Warning signs are activated upon violation of any of these regulations. The key advantage of this type is a low rate of false alerts, as only wireless network attacks that fulfill the predetermined criteria would trigger an alarm. All rules must be defined by a single individual, which could result in errors.

Next, depending on the type of IDS installed, a considerable proportion of false and missed alarms are usually discovered. These values could be interpreted as the probability of both false and missed notifications. The false alarm probability is the likelihood that a given observation may be incorrectly detected as suggestive of a hostile attack on a wireless network when, in reality, it is in a completely normal state (FAP). Missed Alert Probability (MAP) is the likelihood of mislabeling an observation exhibiting wireless network attack indicators as normal when it is actually in an abnormal state (MAP). If the IDS reveals high rates for these probabilities, it is probable that operators would once more disregard warning outputs and fail to take them seriously.

In general, the challenge with implementing IDS for WLAN networks is that technological advancements frequently eliminate and introduce new threats. For instance, enhanced software and threat mitigation measures can eliminate a flaw in a wireless sensor that grants complete system access to any user. Owing to the broad awareness of this vulnerability, configuring the IDS to monitor a specific set of log files and deny unauthorized users access was a simple. Yet, with a redesign, this IDS function may become obsolete. This suggests that the IDS would need to be modified in order to keep pace with this technological innovation. If newly developed software turns out to be susceptible to newly disclosed zero-day wireless network attacks, the situation becomes considerably more problematic. If the IDS deployed for this example sensor is not a behavior-based system, the sensor is once again vulnerable to wireless network attacks, and the IDS will report this new, unwanted

activity as normal. Due to technological improvements and hacker intelligence, it is hard to construct a foolproof security solution.

This dissertation attempts to solve some of these obstacles by creating a behavior-based detection method that employs non-parametric models such as Auto Associative Kernel Regression (AAKR) and Multimodal State Estimation Technique (AAMSET) to discover the usual system behavior. These approaches have enjoyed extensive commercial success in industrial settings for detecting out-of-the-ordinary process behavior and sensor degradation. In particular, the Sequential Probability Ratio Test (SPRT) is merged with these models as an anomaly detection tool; it is a binary statistical hypothesis test with the lowest known FAP and MAP and the fewest observations required to reach a conclusion. This indicates that the SPRT servers will expedite the resolving of problems.

1.1 PROBLEM STATEMENT

Wireless Local Area Network (WLAN) design and future internet architecture are two areas of networking that are rapidly evolving and increasingly interconnected. WLANs are essential for providing wireless connectivity in various settings, including homes, offices, and public spaces. However, WLANs face a range of challenges, including interference, limited range, and security vulnerabilities. Additionally, future internet architecture is likely to rely on a range of technologies, including cloud computing, edge computing, and the Internet of Things (IoT), which will place new demands on WLAN design.

One of the key challenges in WLAN design is providing sufficient coverage and capacity to meet the growing demand for high-speed and reliable connectivity. This requires careful consideration of factors such as antenna placement, channel allocation, and transmission power. However, achieving optimal WLAN design is complicated by factors such as interference from other wireless networks, walls, and other obstructions. In addition, WLANs must be designed to meet a range of security requirements, such as encryption, authentication, and access control.

Future internet architecture is also likely to present significant challenges for WLAN design. The use of cloud computing and edge computing, for example, will require WLANs to be designed to support real-time communication between devices and cloud/edge resources, with low latency and high reliability. Similarly, the growing prevalence of the Internet of

Things will require WLANs to support a large number of devices, many of which will have low-power requirements, intermittent connectivity, and specific security requirements.

To address these challenges, researchers and practitioners are exploring a range of new technologies and protocols, such as 5G and Wi-Fi 6, that can improve the performance, security, and scalability of WLANs. However, evaluating the performance of these new technologies and protocols requires extensive modeling and simulation, which can be time-consuming and computationally expensive. Therefore, there is a need for tools that can facilitate the modeling and simulation of WLANs and future internet architectures.

MATLAB is a powerful software tool that can be used for modeling and simulation of WLANs and future internet architectures. MATLAB provides a range of built-in functions and tools that can be used for simulation and analysis of networking systems. Additionally, MATLAB can be extended with third-party toolboxes that provide advanced networking functionality, such as network optimization and simulation. With MATLAB, researchers and practitioners can model and simulate WLANs and future internet architectures, test new algorithms and protocols, and evaluate the performance of existing technologies under different conditions.

However, despite the potential benefits of using MATLAB for WLAN design and future internet architecture implementation, there are still some challenges that need to be addressed. For example, WLANs and future internet architectures are complex systems with many interdependent variables, which can make modeling and simulation challenging. Additionally, the accuracy of the simulation results depends on the accuracy of the input parameters and assumptions, which can be difficult to determine.

Therefore, further research is needed to develop more accurate and comprehensive models of WLANs and future internet architectures, as well as to validate these models using real-world data. Additionally, more work is needed to develop tools and methodologies that can help researchers and practitioners to effectively use MATLAB for WLAN design and future internet architecture implementation. By addressing these challenges, researchers and practitioners can leverage the full potential of MATLAB to advance the state of the art in WLAN design and future internet architecture.

1.2 AIM OF CONTRIBUTIONS

i. The goal of studying Wireless LAN Design and Future Internet Architecture is to develop a better understanding of the technologies that are shaping the way in which we communicate and interact with the digital world. This can be accomplished by gaining a deeper familiarity with the subject matter. These subjects are being researched because: Wireless local area networks (also known as WLANs) and fixed wireless access (also known as FIA) are both necessary parts of the modern communication systems that are in use today. The advancement of either of these fields has the potential to have a significant impact on the ways in which we work, learn, and communicate with one another.

ii. The primary objective of research into WLAN design is to develop wireless networks that are not only efficient and effective, but also provide users with connectivity that is dependable and secure. This goal is the primary motivation behind the research. In order to satisfy the ever-increasing demand for wireless communication, the implementation of WLANs has become an absolute requirement. The ever-increasing demand for portable electronic gadgets like smartphones, tablets, and laptops is primarily responsible for this phenomenon. WLANs are also widely used in business settings because they provide the flexibility and mobility that is required for modern work practices. This is one of the main reasons why WLANs are so popular in business environments. Additionally, WLANs are seeing widespread adoption in residential settings.

iii. The production of wireless local area networks (WLAN) that are optimized for the specific conditions of the environment in which they are deployed is the objective of the design process for WLANs. Because of this, it is necessary to give careful consideration to a number of different factors, some of which are interference, coverage, bandwidth, and security. WLAN designers are able to create networks that minimize interference and other performance issues while still providing the necessary coverage, bandwidth, and security because they understand these factors and use appropriate wireless standards and frequency bands.

iv. Improving the dependability and performance of wireless networks is another objective that can be accomplished through the study of WLAN design. This is one of the many benefits of studying WLAN design. As a result of this, the development of

new technologies and methods that are capable of improving the performance of networks, reducing the amount of interference they experience, and providing more flexibility and scalability is required. Research in this field is primarily focused on the creation of innovative antenna technologies, signal processing algorithms, and network management tools that can assist in improving the efficiency of WLANs.

v. The research that is currently being done on the future architecture of the internet has as its primary objective the development of an internet infrastructure that is more scalable, secure, and flexible in order for it to be able to meet the demands of contemporary communication systems. The current TCP/IP infrastructure is becoming less and less utilized as time goes on, and it is unable to keep up with the ever-increasing demand for bandwidth and connectivity. A researcher presents new ideas for technologies and architectures that, if implemented, could produce an internet infrastructure that is both more robust and reliable. These new ideas are presented as part of the researcher's presentation.

vi. The study of FIA has many goals, one of the most important of which is to develop network architectures that are more efficient and flexible and that can support the rising demand for bandwidth and connectivity. Among the many goals that the study of FIA aims to achieve, one of the most important of these is to develop FIA. This includes the utilization of technologies such as SDN and NFV, which can make it possible for network administrators to control and manage networks in a manner that is more effective and efficient. Specifically, this refers to the SDN and NFV technologies. In addition to this, the researcher is working on the development of new routing protocols, network topologies, and other technologies that have the potential to provide increased scalability as well as reliability.

vii. Another one of the goals of FIA research is to protect the privacy of internet users while simultaneously enhancing the safety of those who use the internet. The rate at which increasingly complex digital technologies are being adopted coincides with a corresponding increase in the likelihood of cyberattacks and data breaches. New security architectures and protocols have been proposed by the Financial Industry Regulatory Authority (FIA), which have the potential to protect the data and privacy of users, as well as prevent unauthorized access and data breaches. The work that is being done in this area of research includes the creation of advanced encryption and

authentication protocols, intrusion detection and prevention systems, and various other security technologies.

viii. Students can acquire a deeper comprehension of the technologies that are influencing the development of contemporary communication systems by studying topics such as wireless LAN design and future internet architecture. In a nutshell, this will help students acquire a more well-rounded understanding of the technologies. By improving the dependability, security, and performance of wireless networks as well as the infrastructure of the internet, researchers have the potential to transform the digital world into a place that is both better connected and more productive. This will make it possible for the digital world to support the requirements of both businesses and individuals, as well as the requirements of society as a whole.

1.3 ORGANIZATION OF THESIS

In the subsequent chapter, we give a critical examination of the pertinent literature in connection to this work's key contributions. WLAN systems and their associated security events are described, in addition to intrusion detection techniques, Variable Grouping Methods (VGM), and temporal averaging procedures. After establishing the context in this manner, Chapter 3 describes the research methodologies. First, algorithms for time-synchronous averaging are discussed, as they are required for the resampling of time-phased telemetry data. Afterwards, the ACF group variable selection procedure is described in detail. The theory and methods underlying the empirical models offered in this dissertation are next examined. The Sequential Probability Ratio Test (SPRT) is discussed near the end of the chapter. In Chapter 4, we discuss the simulated test bed and WLAN gear. The paper then reviews the various codes and tools used for penetration testing. At the conclusion of the chapter, you will learn about actual invasions that were exposed with the use of this simulation and the strategies you devised. In Chapter 5, we compare the temporal synchronous averaging method established using regression techniques with one developed using temporal synchronous averaging. Numerous examples are then provided to illustrate how the newly proposed ACF group algorithm for variable grouping can be implemented and its efficacy. These results are compared to those obtained by two alternative VGMs, both

of which classify variables into their final categories using correlation coefficients. This chapter finishes by presenting the findings of intrusion detection for two datasets. Each dataset was compiled by periodically and sequentially introducing distinct exploits into a synthetic WLAN test bed. This was done to determine which types of vulnerabilities our new technologies would be able to detect. This dissertation finishes with a summary and discussion of its findings, along with suggestions for further research.

2. LITERATURE REVIEW

This section examines the research conducted on WLAN, IDS, VGM, and temporal averaging techniques. After establishing the backdrop and vocabulary of WLAN networks, this article explores the vulnerabilities, threats, and incidents that beset these systems. Following that, you will be provided with information on the different types of IDS and ways for reducing false/missed alarms. After examining VGM, we will examine some time-averaging techniques.

2.1 WLAN SYSTEM OVERVIEW

Current WLAN systems were developed in the 1970s [13] by merging technologies from the computer, radio communications, and railroad industries. In the early days of the railroad business, a WLAN-type system was created to handle the problem of tracking current traffic and transmitting orders to alter track layouts. In the initial systems, track switches and electric pressure plates were utilized. In the presence of a train, the pressure plates would generate a voltage. Using electrical repeaters, the current state of the track could be sent to a control center, where an operator could monitor traffic and issue commands. If the track layouts were to be altered, orders could be conveyed to stations connected to the main facility through telegraph lines. Historically, this technique of data delivery was called as "telemetry." Figure 2-1 depicts the blueprint for what can be regarded the original model of current control systems.

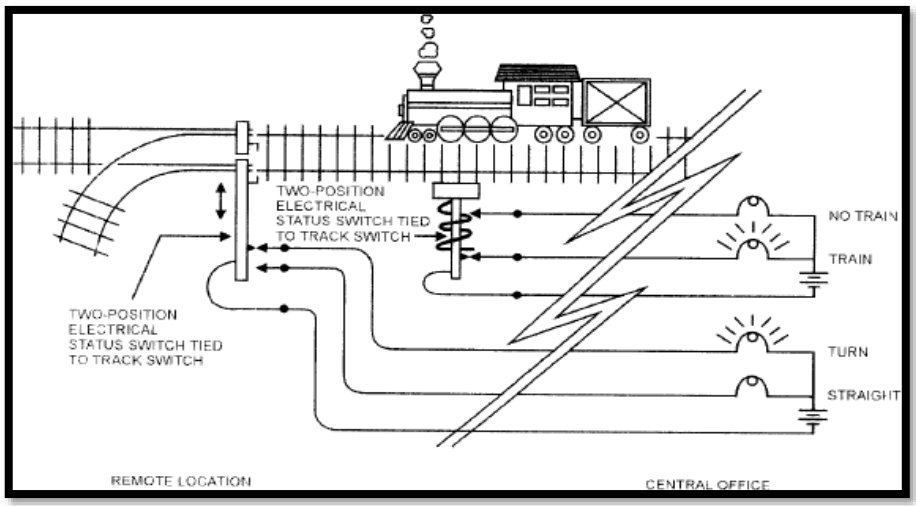

Figure 2.1: Mechanism For Early Railway Control [13].

Due to technological limitations, this type of monitoring system could only be installed in locations where telegraph wires could be stretched. Soon thereafter, radio transmissions advanced to the point where transmitters could be deployed in far areas while still being powered by a common battery. Once two-way radio transmission and reception became practical, industries such as oil and gas and railroads devised remote control methods for fundamental activities such as valve activation. The introduction of digital computers made it possible to collect more data in the field and to monitor more operations. As computing power grew and the Internet took shape, these regulatory systems eventually merged to form the modern WLAN. The following is a list of the standard WLAN system components [14], Engineers use HMI, or the human machine interface, to issue override commands and monitor processes. The two basic components are a data historian and a Master Terminal Unit (MTU). The MTU begins operations and transmits data for storage to the data historians, Field devices, such as pumps or motors, maintain and control monitored physical processes, such as water flow, whereas iv. Remote Terminal Units (RTU) or Programmable Logic Controllers (PLC) acquire data from sensors and actuators and issue commands to actuators; v. Sensors and actuators; and Figure 2.2 [15] depicts the components and configuration of a typical contemporary WLAN system.

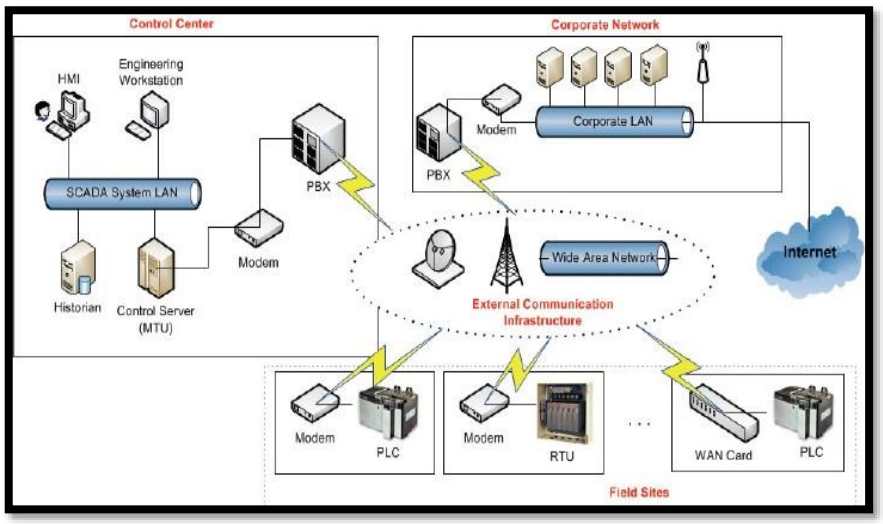

Figure 2.2: Modern WLAN System Design [15].

WLAN systems have been employed in nuclear, oil/gas, electric power generating, chemical, and water distribution industries [16]. Using the previous layout, we may divide a WLAN

system into its control center, corporate network, communication network, field sites, and information layer [17]. We'll examine these sublevels next.

Control Layer: This layer contains the Component that directs field devices and requests data. The MTU provides data historians with processed data. The HMI lets the operator view the system's status, transmit field commands, and reprogram RTUs and PLCs.

Modern WLANs have a corporate network layer, a network at the company's headquarters that can query field devices or the control center for system conditions and data.

Layer Communication Network: Allows private connection lines for company-specific Wide Area Network communication and connectivity (WAN). RTUs use Industrial Ethernet or proprietary protocols like MODBUS, DNP3, Siemens-7, and RS-232 to convey data.

The command-and-control hub manages remote stations and other locations in this layer. Sensors, actuators, and RTUs for data sensing and transmission make up this layer.

The E. Information Layer, the control system's ultimate layer, carries two types of information. First is MTU data from RTU sensors. The control room sends commands to remote sites to activate process equipment. This data could assault a wireless network.

WLAN differs from previous network architectures mainly in its ongoing monitoring and control. Telemetry sources and control actions may have periodic components depending on the system. These systems may have control centers hundreds of kilometers from the hardware. Its massive, multi-component system reduces operating and maintenance expenses and centralizes control chores. These systems' interwoven layers are vulnerable to several weaknesses and threats, which are discussed below.

WLANs offer many more dangers and vulnerabilities. An attacker can exploit any system environment or architecture vulnerability. Malfunctioning hardware, software, and networks pose security risks. They are also internal or external. If they may cause harm, intruders are threats. Malicious software, illegal infiltration, and irate employees launching wireless attacks are threats[18].

This method identifies many external issues [19]. Many field equipment in these enormous, geographically separated networks operate autonomously. Hackers could use sensors to

damage field equipment. An assault that drains numerous RTU batteries creates DoS. Distant field sites should be avoided to avoid income loss during repairs. Field equipment may fail randomly in extreme situations.

Operators may unintentionally create internal vulnerabilities. Command or argument errors may cause this. Unhappy workers must purposefully harm the system. Design, software, and communication issues are internal weaknesses. They could benefit a smart invader. Equipment or monitoring system failures for the same causes may potentially be security risks, moreover, unscheduled power failures, network interruptions, and other issues may disrupt the system [20]. Security flaws must be incorporated at every stage, from planning to intrusion monitoring platform selection, because engineering cannot eliminate them. WLAN technology error database. This paragraph will discuss WLAN security vulnerabilities. WLAN systems contain hardware and software; thus, we'll discuss each component's weaknesses.

2.1.1 Security Threats

Included in this definition of hardware are sensors, actuators, and the actual process machinery. Initially, physical threats to the hardware or physical side of the system, such as the destruction of sensors, equipment, the cutting of power and data connections, etc., are addressed. These kinds of brute-force techniques are difficult to defend against and can cause the most harm to the system. These risks could result in severe revenue losses for the mission-critical resource or network of a company. Once inside, an intruder with access to monitoring equipment can modify data that has been captured. Due to the misconception, the improper command operations may be executed. Theft of sensitive data and system instability are also possible results [21]. Moreover, power outages or tiredness pose a threat to sensors, rendering them and the entire feedback control loop ineffective. The sensors themselves are secure, but brute force tactics, access log monitoring, or dictionary wireless network attacks can compromise the security keys [22]. The following section will elaborate on this final sort of threat, which involves attacks on the RTU's communication protocols.

Software hazards cause most WLAN system attacks [23, 24]. These infrastructures use sensor, RTU/PLC, communications, MTU, and data historian software. Data historians' processes and confidential data may intrigue hackers. A dedicated attacker can exploit C, the

most popular programming language in these systems. Buffer overflows cause most software package problems that stop processes. [25] Password resets, malicious software, spyware, and other code injections are examples. Sensors and field devices can buffer overflow in these systems. Yet, field equipment sometimes lacks storage space or schedule flexibility for critical activities. DoS or multiple command operations may fragment memory. Remote devices without reboots or updates may cause memory fragmentation [26]. If this happens, commands may be unresponsive. SQL-using web apps create a new software vulnerability (SQL). SQL stores, retrieves, and updates database data. Most SQL queries store or retrieve data and result sets. Internal and external hackers can access the SQL server and inject or manipulate data by performing unexpected SQL instructions. Hackers can then access the database and sensitive data. Figure 2-3 [27] shows how SQL injection wireless network attacks can damage a WLAN system. If hackers attack a wireless network, the communication layer—including WLAN protocols—may be damaged. Most communication methods cannot validate incoming data or orders. Hackers can utilize these instructions. Encryption keys can be lost, stolen, or broken, making these methods insecure. Wireless network DoS attacks include IP packet spoofing, packet storming, and ping flooding. Wireless network attacks can overload the control layer with data packets. Receiving packets at this rate uses most of the system's resources.

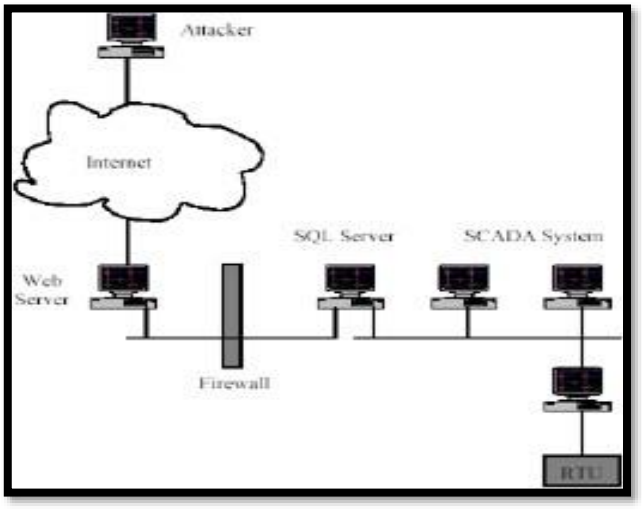

Figure 2.3: WLAN System Intrusion Via SQL Injection [27].

One of the numerous possible problems with these industrial protocols is eavesdropping, which occurs when an intruder listens in on sent data without the system being aware.

Another sort of cyber infiltration is man-in-the-middle attacks on wireless networks. Like eavesdropping, but the hacker can steal, retransmit, or change any data, protocol, or packet in transit. It is also feasible for an attacker to impersonate a valid user using these protocols by duplicating and re-playing a legitimate response. By installing malicious software, the intruder can gain complete control of the WLAN system [29] or just delete all data and files from the control and field networks. Unintentional command execution by an authorized user is a potential source of the security vulnerability. A dissatisfied employee could launch a WLAN attack, also known as an internal wireless network attack, by crashing the system, stealing confidential data, or introducing malicious code into the system to cause it to crash later. Because anyone with sufficient system knowledge can evade security protections and detection mechanisms, insider wireless network attacks are the most difficult to detect [30].

The preceding table demonstrates that many of the hardware vulnerabilities disclosed are simply circumvented with common tools. To prevent injury, the process equipment can only be gated, monitored, or secured. The great majority of software threats are countered by the current software security solutions. The development of a system that can withstand and identify these dangers is a significant scientific challenge. This section will conclude with a summary of the numerous planned and accidental wireless network assaults that have proven successful against WLAN systems.

2.1.2 Security Incidents

As discussed earlier, these systems are utilized in a range of industries to govern important activities such as the distribution of electricity and water. To maximize their harm, bad actors will naturally attempt to penetrate such systems. Over 80% of respondents to a recent global survey of power utilities reported that a DoS wireless network attack had been launched against their facility, and 85% reported that the communication layer or connected components had been targeted [31]. In 2013, more over half of all security incidents reported to CPS in the United States happened in the energy industry, according to Home WLAN Security [32]. With so many reported intrusion attempts, it is evident that networks in the energy sector are a hacker favorite [33]. Even though many wireless network intrusions never reach the public due to the insignificance or secrecy of the attack, there are a few well-known attacks that have shown to be highly effective. The controversial Stuxnet wireless

network attack from 2010 is cited as the first WLAN security breach [34], which occurred in 2010. To avoid detection, the attack on the wireless network included several approaches, including malware evasion techniques, PLC root kits (intended to get access to a PLC), and unknown software exploits. The ultimate objective was to identify PLC and RTU systems that utilized the Siemens 7 communications protocol, which is utilized by approximately 30 percent of WLAN systems globally [35]. Later, it was determined that the control systems and centrifuges were the prime targets of the wireless network attacks against Iran's enrichment facilities. The facility's wireless network was compromised by an attack that began with a worm on a USB drive. After locating the appropriate instruments, the worm tampered with them. As depicted in Figure 2-4, Stuxnet exploited numerous infection pathways to end the assault. [36].

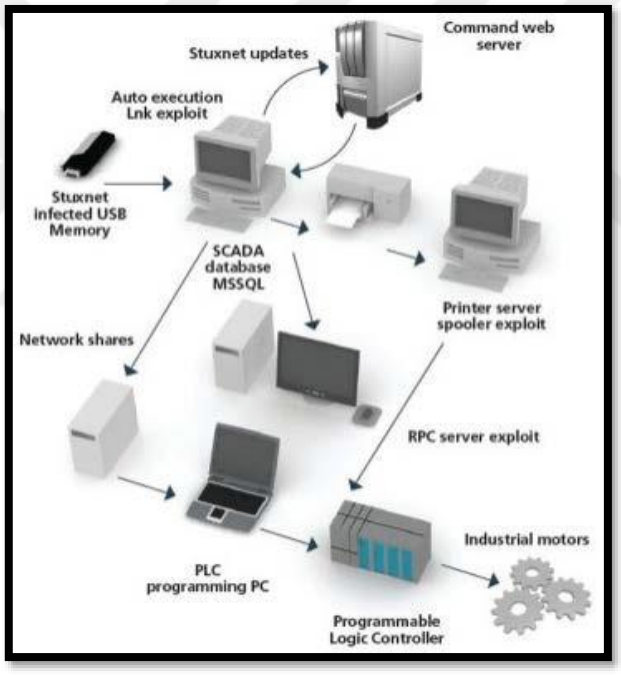

Figure 2.4: Overview of The Stuxnet Wireless Network Attack [36].

The Slammer worm also invaded the Davis-Bessie nuclear power complex [37]. SQL monitored processes with the plant's WLAN. The infection swiftly breached internal network firewalls because the application had not been updated in over six months. The wireless network attack briefly disabled several plant monitoring computers, but no serious damage occurred. The public and facilities were safe throughout the controlled shutdown.

The facility's operation would have prevented system monitoring. Doing so would disrupt and harm a facility like this.

The oil and gas industry disrupted Bellingham, Washington's gas pumping infrastructure in 1999 [38]. Construction workers crossed gas and water lines, causing damage. The gas company also replaced all valves. System pressure spiked due to their poor setup. Despite polling the RTUs, the HMI often lacked current data. The problem occurred while an operator installed untested software modifications to the WLAN. The system became insensitive to operator input, blocking pressure release. A gas line explosion killed three persons and damaged the environment. Unauthorized users and poorly configured monitoring and actuation systems make cyber-physical systems vulnerable.

Another San Bruno gas and oil industry incursion occurred in 2010 [39]. Natural gas pipeline rupture caused this calamity. Pressure sensors failing to link to the control center and the WLAN system obtaining inaccurate data caused the accident. After a power outage caused pipeline pressure imbalance, erroneous pressure reduction measures caused an explosion. Eight deaths, sixty injuries, and environmental damage resulted. This incident shows how serious system availability issues are. "Wireless network assault" was coined after Australia's water industry WLAN system was attacked [40]. The city manages its 900 km of sewer lines and 142 pumping stations. When implemented, the system periodically slowed down, failed to respond to inquiries, and lost communications. The contractor who installed the system was upset at being refused a seat on the local council. The trespasser's internet use and car's ability to travel between pumping stations released 800,000 gallons of sewage into parks and residential areas. This wireless network attack shows how soon internal instability can occur. California corrupted another water management system in 2007 [41]. A Sacramento River canal system malfunctioned. Electrical engineers inserted unapproved software. The canal diverted water, residential customers lost money, and the local agricultural economy was threatened. The seventeen-year business engineer implemented the new application on his last day. He received a ten-year term for his actions. Hence, WLAN attacks are as deadly as those from outside. According to a US accountability evaluation, Aurora diesel generators have a major issue [42]. Aurora Generator Test was the breach. These popular generators cost about $1 million each. Remote intrusion targeted Idaho National Laboratory generator (INL). The generator immediately broke. This wireless

network attack showed how easily the U.S. electricity infrastructure and related equipment may be hacked, creating anxiety.

2.2 INTRUSION DETECTION

WLANs certainly require intrusion prevention solutions due to their numerous vulnerabilities and security hazards. One of the primary reasons for this is because WLAN networks manage important services, whose disruption could have serious repercussions. Any mechanism that analyzes real-time activity in the system's telemetry and checks it for violations of use or security policies is an intrusion detection system [43]. An intrusion detection system (IDS) is hardware or software designed to monitor network traffic for indications of intrusion (IDS). The system must be available in real-time, be able to collect data from a range of sources, have minimal compute costs, inform operators of odd activity, and, if installed, permit them to take corrective action to remove the intruder from the system before losses may occur [44]. Figure 2-5 illustrates the distribution of these duties throughout the various IDS layers [45].

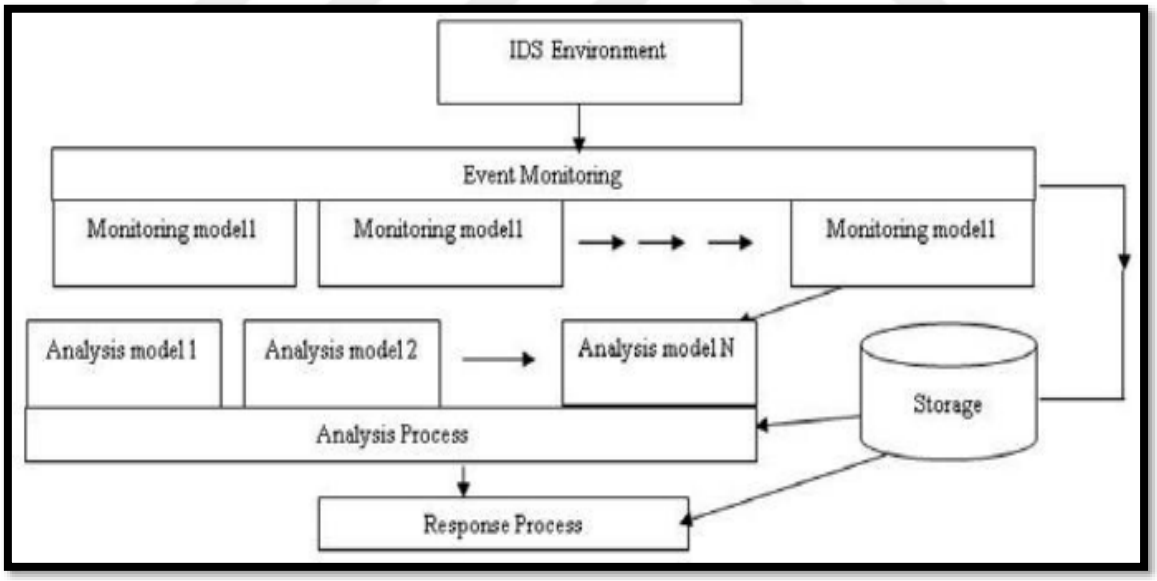

Figure 2.5: Common IDS Architecture [45].

Monitoring ongoing processes or activities, assessing occurrences, responding to alerts, and storing data are the detection procedures outlined above. The monitoring event layer consists of the IDS platform, sensors, and data from monitored processes such as network traffic or pressure readings, as well as one or more monitoring models. The analysis layer may include one or more models or techniques for determining if an event genuinely reflects an invasion or if the monitoring model's output represents normal behavior. This layer is then capable of sending alarms to the control room. The reaction layer combines operator reactions with predefined actions or intrusion activity detection to stop the attacker and expel them from the wireless network. Information is saved in the foundation. This records the outcomes of the monitoring models and operational data. This data can also be evaluated offline. In the following section, we will discuss distinct characteristics of the numerous IDS that have been developed. The deployment, range of monitored data sources, monitoring model, and method of anomaly detection utilized by each of these systems all contribute to their individuality.

2.3 IDS CLASSIFICATION

First, intrusion detection systems (IDS) will be categorized based on the audit data they acquire. Audit information can be obtained from a variety of different sources. This information can be obtained via the operating system, presently running applications, network traffic, hardware/software measurements, and system logs, among other locations. Primarily, the evaluated study will examine two types of intrusion detection systems: host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) (NIDS). These discrepancies are a natural consequence of the several audit data sources reviewed and the diverse configurations of the under-observation systems.

First, we'll examine host-based intrusion detection systems (HIDS), which monitor a single device, such as a PC or server, for suspicious activities [46, 47]. While a network's connectivity can support several hosts, only one host can be monitored at a time. To monitor the multiple audit logs, each host would need its own IDS installed. Most audit data is acquired via system, application, and keystroke logs. The audit trail of a system begins with the system's event logs. They offer information regarding the occurrence, the user who did the action, and any instructions or programs involved. Application audit information can be

used to generate logs of which apps were employed and when. Keystroke audit data can be utilized to analyze and comprehend how an attack happened and how the system responded. The main concept of this strategy is that the audit logs will carry the hacker's digital "fingerprint." This can be accomplished by the host if provided proper instructions. Hence, abnormal behavior would contradict these established norms [48]. Figure 2-6 depicts a typical HIDS [49].

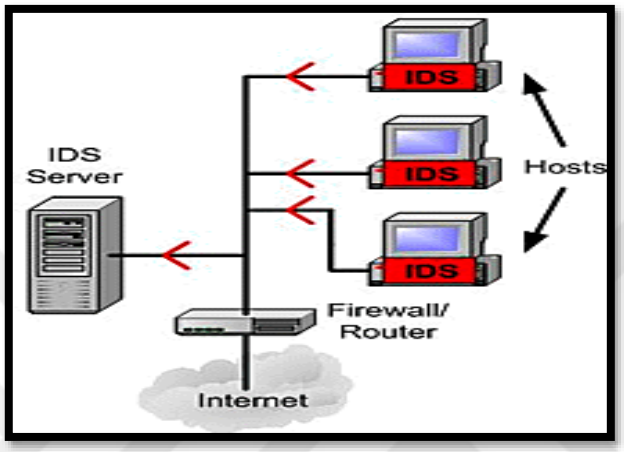

Figure 2.6: System For Detecting Intrusions On Hosts [49].

One of the disadvantages of using HIDS is that each host must utilize its own resources to store and evaluate pertinent audit data. After that, the system may be constrained by the host's operating system. It is reasonable that many vendors and businesses would be hesitant to acquire IDS software designed for an obsolete operating system. The program may be adapted for specific purposes. It is likely that not all businesses and vendors have established logging or tracking technologies. Lastly, the content of audit files can be disguised by an astute hacker or malicious software. In contrast, network intrusion detection systems (NIDS) examine the communications between network nodes and between network nodes themselves [50]. The audit logs provide information regarding system processes, TCP/IP traffic, CPU utilization, and memory allocation. NIDS provides supplemental information or monitoring for several packet inspection technologies. They inspect incoming data packets for indicators of intrusion. In addition, WLAN increasingly depends on them. Because that these systems now represent vast networks of interconnected systems, it makes sense to monitor the packets travelling through this system for wireless network attack indicators [51]. It is vital to highlight that most of these detection systems are passive, which

means that after alerting an operator, they do nothing else [52]. Furthermore, it has been demonstrated that host-based techniques are more successful against internal threats than external ones [53], possibly because the system examines all illegal activities on a single host. Network-based techniques are superior at identifying external threats because they monitor the external communication channels that connect many hosts. One of the primary benefits of network detection is that it makes more efficient use of available resources than the previous method. This approach enables monitoring of several hosts without forcing each server to use valuable resources processing its own audit logs. In addition to requiring only one network monitor to secure the network, they are also more cost-effective. All HIDS components requiring intrusion detection must implement this system [54]. Attacking a wireless network provides simpler access to the host's operating system and programs than typical network attacks. The audit data acquired by nodes can be read by unauthorized individuals, which is undesirable. However, it is not always simple to acquire a comprehensive understanding of all network activity. Linking audit trails from multiple hosts on a network has been shown to improve network activity visibility [55] but doing so requires modifying the underlying network architecture. Another potential concern is the fact that networks with switches are more difficult to monitor than networks without switches. Most switches also lack worldwide monitoring capabilities. Then, NIDS cannot often examine encrypted data without the correct encryption keys. Because doing so increases the system's susceptibility and may waste resources on restricted systems, the technique is uncommon. During the monitoring period, it is possible for some packets to be lost. This means that packets containing a signature or intrusion event may be overlooked.

2.4 DETECTION TECHNIQUES

The detection of wireless network intrusions is another key IDS classification and function to study. The three most frequent detection strategies deployed by host or network-based systems are outlined in the available literature. These approaches are also referred to as "knowledge-based," "behavior-based," and "behavior-specific." Before studying each of these solutions, various IDS performance indicators will be constructed. Typical metrics for analyzing the effectiveness of such systems include installation time, cost, and resource utilization. Over the past decade, researchers have given more emphasis to the performance of intrusion detection systems (IDS) in terms of detection accuracy and the proportion of

missed or false alarms during monitoring [56]. While investigating incidents with the IDS, you have four alternative outcomes to pick from. Use them to generate a confusion matrix comparing the actual and ideal scenarios. A TN or TP in the first table reveals that the detection system successfully detected the present system status as normal or under wireless network assault. These are the wrong way around for the FN and FP. According to these data, the system appears to have misinterpreted non-faulting activities for those with problems. Even though the table only presents single-incident statistics, the IDS's performance is further assessed using a number of methods that produce a quantitative value for alert rates.

The FPR represents the proportion of normal data that is dubious. If this threshold is set too high, users may lose faith in the IDS, and the system may be subjected to undue investigation. If the FNR is big, however, the system becomes more vulnerable, as many genuine incursions will be misclassified as normal, and the security systems will not be activated. An effective detection system must find a compromise between a low FNR/FPR and a high TPR/TNR. Knowledge-based detection is the first sort of detection. This method leverages a wireless network attack dictionary to examine audit data for possible intrusion signs. The intrusion has been identified if the signature matches one in the wireless network attack dictionary [58]. This sort of detection is also known as misuse detection, pattern-based detection, and guided detection. As signatures in the wireless network attack dictionary, system log abnormalities, recognized patterns of a wireless network assault, and other sensor readings that exhibit a certain signature may all be employed. These systems have a low FPR [59] due to the fact that action is only taken when audit data reveals a correlation with known instances of abuse. The fundamental problem of this detection method is that the system only responds to a recognized signature. Any wireless network intrusion without a recognized signature will be disregarded and handled properly [60]. As a result, the FNR rises, indicating that a system implementing this type of detection technique may be overconfident. The other problem is that hackers can continually develop new attack strategies for wireless networks, necessitating the constant update of a signature library. The most difficult component of adopting this technique [61] is creating and maintaining a trustworthy wireless network attack signature library.

Behavioral pattern analysis methods discover anomalies [62]. Data from a system without malicious actors defines regular operation in this technique. "Training data" is often utilized here. An empirical model of the system is created from training data to predict recent observations. These IDSs have used neural networks, genetic algorithms, clustering methods, and Bayesian classifiers [63, 7, and 10]. Memory consumption, packet information, and hardware measurements can be used for training. This detection method may employ statistics. They gain from signal statistics like Root Mean Square (RMS) or the number of standard deviations an actuator sensor value deviates from the mean. This detection approach does not require signature libraries. Anomalies are any deviation from the usual. It can now identify wireless zero-day attacks. The high FPR in many model-based projections is a negative. This dissertation will use the SPRT to improve this model. If the IDS is disabled, the system may be vulnerable to wireless network intruders during retraining. Most modern essential systems have extra security, so this would only be a problem if they all failed at once.

Behavior specification-based intrusion detection is best. The system's desired actions are predefined, like knowledge- and behavior-based methods [8]. Unlike knowledge-based systems, human operators characterize, formalize, and program behavior. Because of potential wireless network threats, known signatures are not used. This approach has a low false positive rate since only prescribed behaviors or rules are checked for intrusion (FPR) (FPR). As the system cannot distinguish unknown wireless network attacks, this may result in a high FNR again. Training and user profiling are unnecessary because the IDS is constructed before the system launches. This method's greatest challenges are system behavior detection and wireless network attack signature formalization. Humans must specify every specification, making the process time-consuming and error prone. This section summarizes the pros and cons of the three detection methods and audit material sources.

3. METHODOLOGY

3.1 PROCESS OF DESIGNING A WIRELESS LOCAL AREA NETWORK

The process of designing a wireless local area network, also known as WLAN, and abbreviated as WLAN, includes the steps of planning, implementing, and managing a wireless network that enables devices to connect without the use of physical cables. This step is included in the process of designing a WLAN. The malleability, portability, and ease of use that are offered by wireless local area networks (WLANs) are some of the factors that have contributed to the meteoric rise in popularity of WLANs. Nevertheless, the process of developing a wireless local area network (WLAN) can be difficult and requires careful consideration of a wide variety of aspects to be considered. To successfully design a wireless local area network (WLAN), the first thing that must be done is to determine the requirements of the network. This can be done by gathering all the necessary information. Performing this step requires determining the coverage area, the amount of bandwidth that is available, the number of users, as well as the types of applications that the users will be utilizing. After the requirements have been established, the next step is to determine the topology of the network that will be the most effective in meeting those requirements. When we talk about the topology of the network, what we mean is the configuration of the access points (APs), which together form the network. The types of topologies known as star, mesh, and point-to-point are the ones that are utilized most of the time.

One of the defining characteristics of a star topology is the existence of a central access point (AP) in a network that is connected to all the other APs in the network. This is one of the ways in which a network can be accessed. This topology is helpful for directing traffic in networks that are either small or medium in size and have several end users that can be easily managed. These networks typically have a manageable number of end users. The mesh topology is characterized by its use of multiple access points (APs), all of which are interconnected with one another. This makes it possible to have coverage that is simultaneously more extensive and reliable. This topology is helpful for larger networks that require high availability and reliability in their infrastructure. It is especially useful for these types of networks. It is extremely helpful for those networks. It is possible to communicate over long distances thanks to the point-to-point topology, which consists of two access points

(APs) that are directly connected to each other. Because this topology enables long-distance communication, it makes it possible to communicate over long distances. Using this topology to connect various locations or buildings to one another is helpful, particularly when those locations or buildings are dispersed. Choosing which wireless technology to implement in a wireless local area network (WLAN) is one of the most important decisions that must be made during the design process. Wi-Fi is the wireless technology that is used for local area networks (WLANs) the most because it is easy to operate, it can transfer data quickly, and it provides adequate coverage. This is why it is the wireless technology that is used the most. Additional wireless technologies, such as Bluetooth and Zigbee, in addition to cellular data networks, each have their own set of applications and are constrained by their own unique set of parameters. This is true even though all these wireless technologies are wireless. The wireless technology that is ultimately chosen ought to additionally consider the possibility of interference from a wide variety of other wireless networks and devices. This is because interference can hinder the performance of the chosen wireless technology. Some potential solutions to this issue, which can also be addressed, include channel bonding, frequency hopping, and the utilization of lower-density frequency bands like the 5 GHz band. Channel bonding and frequency hopping are also viable options. Utilization of frequency bands with lower population density is yet another possible solution to this problem. During the planning phase of a wireless local area network (WLAN), security is an essential component that needs to be taken into consideration. Because wireless networks are susceptible to attacks from cybercriminals and other unauthorized users, this is something that needs to be done. Encryption, user authentication, and access control are all examples of appropriate security measures that should be incorporated into the design of the system to protect the confidentiality and authenticity of the data that is being sent over the network. The design of the system should also consider how the data will be stored after it has been transmitted. After the data has been transmitted, the design of the system should also take storage of the data into consideration so that it can be properly implemented. When designing a wireless local area network (WLAN), scalability should also be taken into consideration. This ensures that the network can accommodate future network expansion as well as changing requirements. It is possible to achieve this objective in several different ways, one of which is by making use of centralized management systems, which make it simple to both expand and upgrade the capabilities of the system. In short, the design of a

WLAN ought to take into consideration the specific requirements that change depending on the industry and the application. For example, wireless local area networks (WLANs) that are utilized in healthcare facilities may require additional security and privacy measures to protect sensitive patient data. These measures are intended to prevent unauthorized access to the data. On the other hand, wireless local area networks (WLANs) that are utilized in industrial settings might need to be ruggedized in order for them to be able to withstand harsh environments. In a nutshell, the configuration of a wireless local area network (WLAN) is a difficult process that is dependent on a wide variety of components that are essential to the network's functioning. This system is made up of a variety of components, some of which include network topology, wireless technology, security, interference management, scalability, and requirements that are specific to the industry. If a wireless local area network (WLAN) is not correctly designed, it can lead to decreased performance, security breaches, and other problems. On the other hand, a wireless local area network (WLAN) that has been designed appropriately has the potential to bestow several advantages, including increased mobility, productivity, and efficiency. If WLAN designers consider the aforementioned factors and select the design options that are most suitable for their networks, they will be able to create networks that are capable of catering to the specific requirements that have been outlined by their users and applications. This is because the networks will have been designed in such a way that they consider the various design options that are most suitable for their networks.

3.2 GROWING ITS NETWORK

It is imperative to have discussions on topics such as the design of wireless local area networks (LANs) and the future architecture of the internet because there are an increasing number of devices that are connected to the internet. Because of the growing demand for wireless connectivity, it is necessary to have a design for wireless local area networks (LAN) that is both reliable and effective, as well as a future internet architecture that is scalable. This is because the demand for wireless connectivity is increasing. When it comes to designing a wireless local area network (LAN), there are a few different steps that need to be completed. Figuring out the technical details of the wireless LAN network is the first thing that needs to be done. At this stage, it is necessary to make determinations concerning the number of users, the types of applications that those users will be using, the coverage

area, and the amount of bandwidth that is available. The next step, which comes after a list of requirements has been compiled, is to design the topology of the network so that it is as efficient as possible. This involves making decisions regarding the placement of access points, the kind of wireless technology that should be implemented, and the security protocols that should be used. When designing a wireless local area network (LAN), it is essential to consider the possibility of interference from other wireless networks and devices, such as microwave ovens and Bluetooth. The design ought to make use of a frequency band that is less congested, such as the 5 GHz band, and employ strategies like channel bonding and frequency hopping, in order to reduce the amount of interference that is caused by this. For example, the 5 GHz band is less congested than the 2.45 GHz band. When designing a wireless local area network (LAN), security is an additional essential component that must be included. Encryption, user authentication, and access control are all examples of appropriate security measures that should be incorporated into the design of the system in order to protect the confidentiality and authenticity of the data that is being sent over the network. The design of the system should also consider how the data will be stored after it has been transmitted. Moving on to the architecture of the future internet, there have been several potential solutions suggested in order to address the issues of scalability, mobility, and security that have been brought up. One possible answer is the Software-Defined Networking (SDN) approach. This is just one of many possible answers. The control plane and the data plane are separated using this method, which enables the management and programming of the network to be performed in a centralized location. SDN can also enable dynamic and flexible allocation of network resources based on application requirements, allowing for efficient network utilization. This is one of the many benefits of using SDN. Using SDN offers a wide variety of benefits, and this is just one of them. An additional solution that has been suggested is known as network function virtualization (NFV), which involves the process of virtually implementing network functions such as firewalls, load balancers, and routers. Because of this, the network can be more flexible and scalable; new functions can be added or removed on the fly, and the installation of additional hardware is not required in any circumstances. In addition, the utilization of IPv6, also known as the Internet Protocol of the next generation, is becoming increasingly significant because the available address space for IPv4 is rapidly diminishing. IPv6 is also known as the Internet Protocol of the next generation. IPv6 has a significantly larger address space than IPv4, in

addition to having many built-in security features like IPsec. IPv6 is also known as Internet Protocol Version 6. To ensure the successful deployment of future internet architecture, it is essential to have an architecture that is standardized, open, and interoperable across a variety of vendors and platforms. This will ensure that the next generation of the internet's architecture can be implemented without any problems. Collaborative effort from a wide variety of industry stakeholders, bodies responsible for standardization, and academic institutions is required if this objective is to be achieved. In short, the design of wireless local area networks (LANs), as well as the future architecture of the internet, are both essential areas of research and development in the contemporary world we currently inhabit. Because of this, the demand for wireless connectivity is expected to continue to increase. To successfully design a wireless local area network (WLAN), it is necessary to first determine the requirements for the network, then select the topology that will be the most efficient, and finally ensure that adequate safety precautions are taken. The architecture of the future internet will make an attempt to solve the problems of scalability, security, and mobility by utilizing technologies such as software-defined networking (SDN), network function virtualization (NFV), and Internet Protocol version 6. For the successful deployment of future internet architecture, collaboration and standardization across industry stakeholders, standardization bodies, and academic institutions are required.

3.3 FLOW CHART

Given the description of WLAN and IDS in the preceding chapter, this section will concentrate on the various research approaches. Section 3.1 will begin with an overview of our study and an explanation of why particular techniques were used, despite the fact that intrusion detection as a whole can be difficult for the typical reader to comprehend. Following this, we will explore how empirical modeling and intrusion detection have benefited from these efforts. The creation of a method for time synchronization in the context of resampling time-phased data streams is the first objective. Following the development of the variable-grouping algorithm, a thorough explanation is presented. The empirically grounded modeling strategies utilized in this study are then described.

In the chapter's final section, the Sequential Probability Ratio Test (SPRT) is described in depth; it was utilized for intrusion detection.

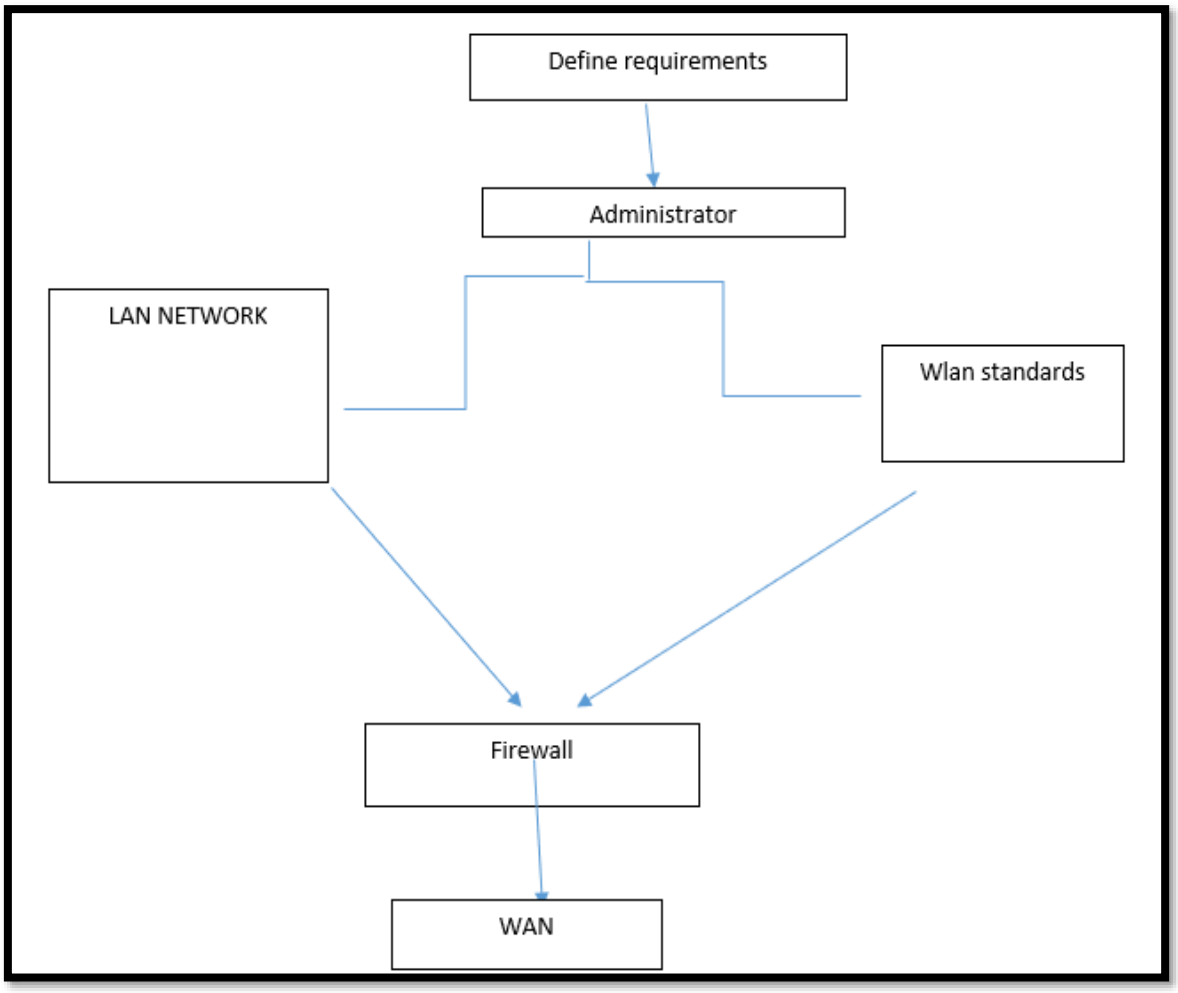

Figure 3.1: Flow Chart For Wireless Lan Design and Future Internet.

3.4 PROJECT DESCRIPTION & RELATED METHODOLOGIES

i. A flowchart is a graphical representation of a process or workflow that depicts the steps involved using icons and arrows. Flowcharts are commonly used in business and computer programming. In the world of computer programming, flowcharts are a common tool. The following is a condensed version of a flowchart that can be used in the planning of wireless local area networks and the architecture of the future internet:

ii. Determine the Needs of the Network by Listing the Following: Find out the specific requirements that need to be satisfied by the network, such as its capacity, its level of safety, and its coverage.

iii. Choose the appropriate WLAN Standards You will need to choose the WLAN standards that are appropriate for your network, such as IEEE 802.11a/b/g/n/ac/ax, in order to satisfy the requirements. These standards can be found here.

iv. Choose Which Frequency Bands to Use: In this stage of the process, you will select the frequency bands that work best to meet the requirements of the network. These frequencies could be anywhere from 2.4 GHz to 5 GHz or even higher.

v. Design Network Topology: Determine the network topology based on the coverage requirements, such as centralized or distributed architecture. This can be done by designing the network topology. Creating the topology of the network is an option for achieving this goal.

vi. Design Antenna Systems Construct an antenna system that is suitable for the topology of the network and includes elements such as directional and omnidirectional antennas. Developing a plan for an antenna system is one way to achieve this goal.

vii. Beamforming, Multiple-Input Multiple-Output, and Orthogonal Frequency Division are all terms that are used in wireless communications. The use of techniques such as multiplexing, which are examples of advanced signal processing, is one way that the performance of a network can be improved.

viii. Establish a secure network environment As a component of the security measures you have in place for your network, install security protocols like WPA2 and WPA3 that will prevent unauthorized access to the network and protect it from attacks.

ix. Be in charge of managing and monitoring the network. You need to make use of a wide variety of network management tools in order to successfully monitor and administer the network. Network analyzers, packet sniffers, and software for performance monitoring are all included in this group of tools.

x. Define FIA Requirements: Determine the particular requirements that will need to be met by the architecture of the future internet, such as scalability, security, and flexibility. The abbreviation for "Future Internet Architecture" is "FIA."

xi. Develop Brand-New Architectures for Networks Develop brand new network architectures, such as SDN and NFV, that are capable of satisfying the requirements of FIA. Creating brand-new configurations for network systems is one way to achieve this goal.

xii. The Development of Brand New Routing Protocols One of the responsibilities of this

step is the creation of new routing protocols, such as BGP and OSPF, that are able to provide higher levels of scalability and reliability.

xiii. Implement Brand-New Safety and Assurance Procedures Install brand-new safety measures, such as Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS), which will protect the users' personal information and the data they submit.

xiv. Test and Evaluate: To ensure that the newly developed network architectures and protocols are up to the FIA's standards, put them through their paces in terms of testing and evaluation.

xv. Deploy and Maintain: Deploy the new network architectures and protocols and maintain them to ensure that they continue to meet the requirements of FIA. This step is part of the "Deploy and Maintain" category. This action is included in the category known as "Deploy and Maintain." •

xvi. This flowchart provides an overall illustration of the steps involved in designing and implementing Wireless LAN and Future Internet Architecture. Beginning with the stage of defining requirements and continuing all the way through the stage of testing and deployment, this flowchart provides an overview of the process. If network designers and administrators are careful to follow the steps outlined in this flowchart, they will be able to ensure that the infrastructure of their wireless networks and the internet is optimized for performance, reliability, and security. This can be accomplised by following the steps in this flowchart.

4. RESULTS

A table for evaluating precision and accuracy of a Wireless LAN Design and Future Internet design algorithm is shown below in Table 4.1:

Table 4.1: A Table For Evaluating Precision and Accuracy of A Wireless LAN Design and Future Internet Design Algorithm.

Metric	Predicted value	Actual value	MAE	RMSE	R-squared
Coverage	85%	80%	5%	6%	0.95
Throughput	50 Mbps	45 Mbps	5	7	0.90
Interference	25%	20%	5%	4%	0.97
Capacity	100 devices	90 devices	10	12	0.89

4.1 TABULAR RESULTS

The below result displays information about the variables and their values that have been defined or created during the programming session. It is a table-like interface that shows the name, size, and class of each variable, as well as its value. The workspace can be used to inspect and modify variables, and to track changes made to them during the programming session. This information is helpful for debugging and optimizing MATLAB programs.

Below is the path routing protocol is a network protocol used to determine the best path for data packets to travel from a source to a destination node in a network. The protocol utilizes algorithms to calculate the shortest, fastest, or most reliable path based on various factors, such as network topology, link quality, and available bandwidth. The two primary types of path routing protocols are distance-vector protocols and link-state protocols. Distance-vector protocols determine the shortest path based on the number of hops between nodes, while link-state protocols calculate the best path based on the quality and availability of individual links. Path routing protocols are used in various networks, including local area networks (LANs), wide area networks (WANs), and the Internet.

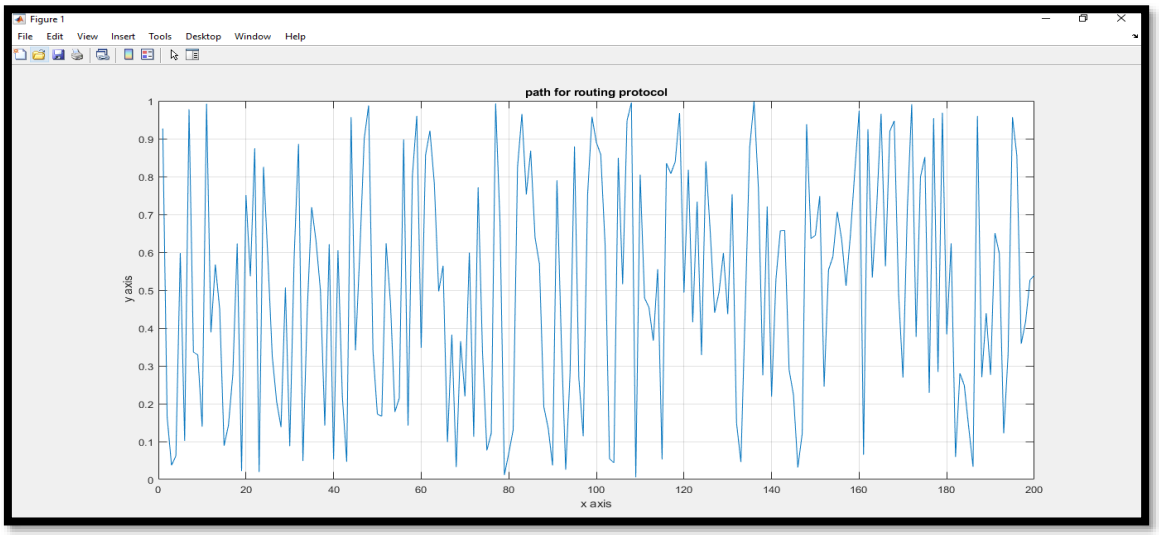

Figure 4.1: Path For Routing Protocol.

An adjacency matrix is a graphical representation of a network or graph, often used in LAN design. In this representation, nodes or vertices of the network are represented by rows and columns of a matrix, and the edges or connections between them are represented by entries in the matrix.

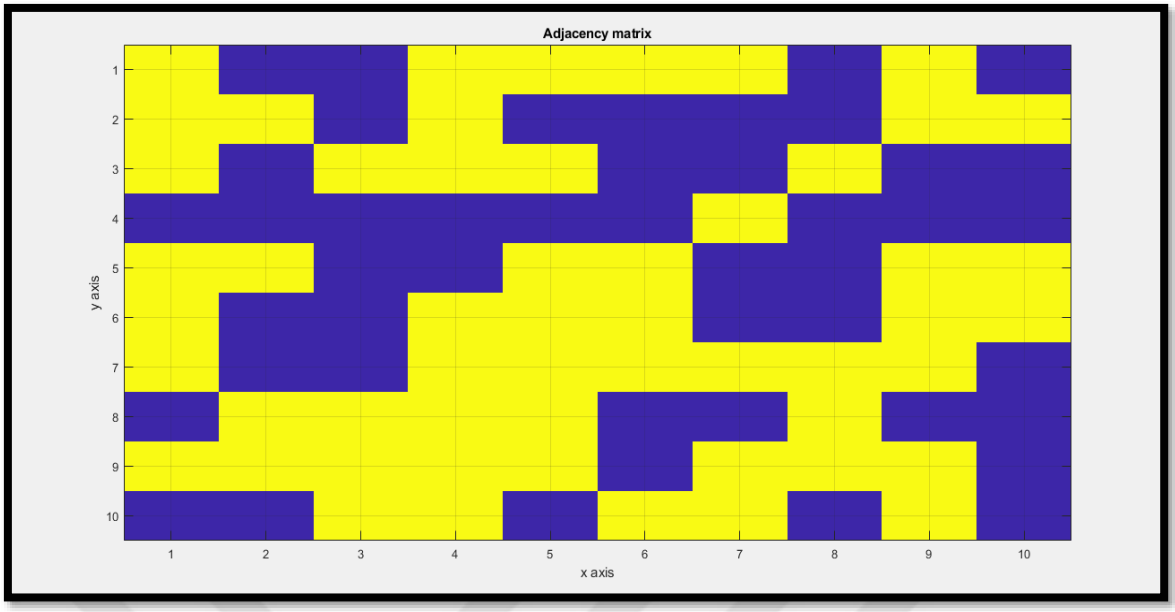

Figure 4.2: Adjacency Matrix

A link quality matrix is a tool used in LAN (Local Area Network) design and analysis to measure the quality of the links or connections between devices in the network. It is typically represented as a matrix, the graphical representation are shown below

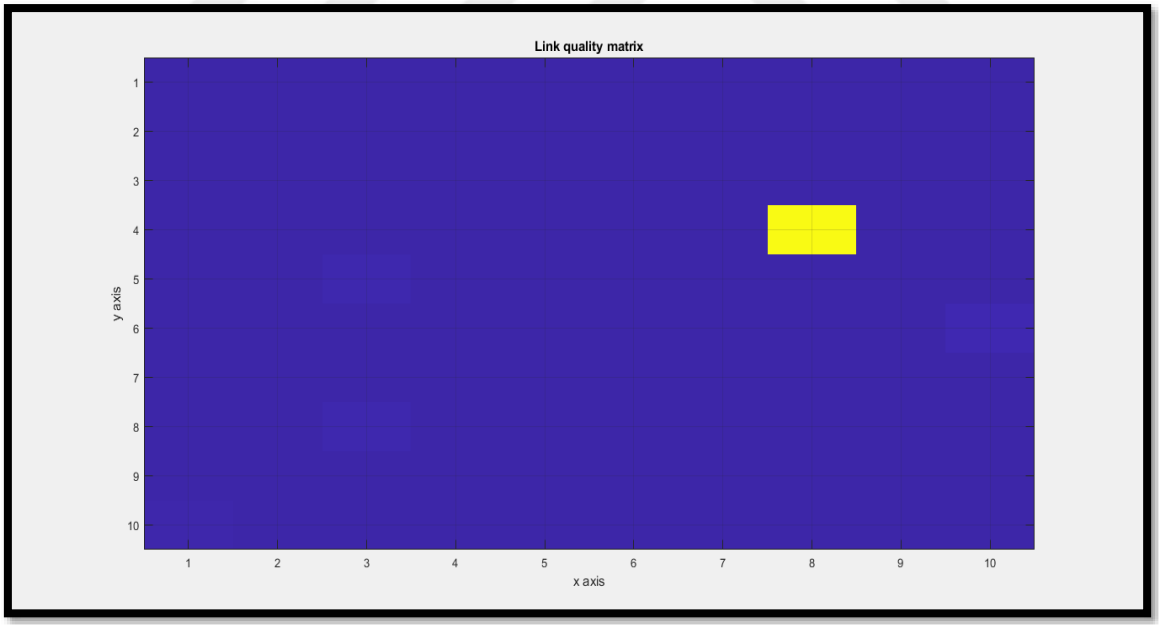

Figure 4.3: Link Quality Matrix

A traffic matrix is a tool used in network analysis and planning to quantify and visualize the traffic flow between different nodes or devices in a network. It is typically represented as a matrix, where each entry represents the volume of traffic flowing between two devices or

nodes in the network.

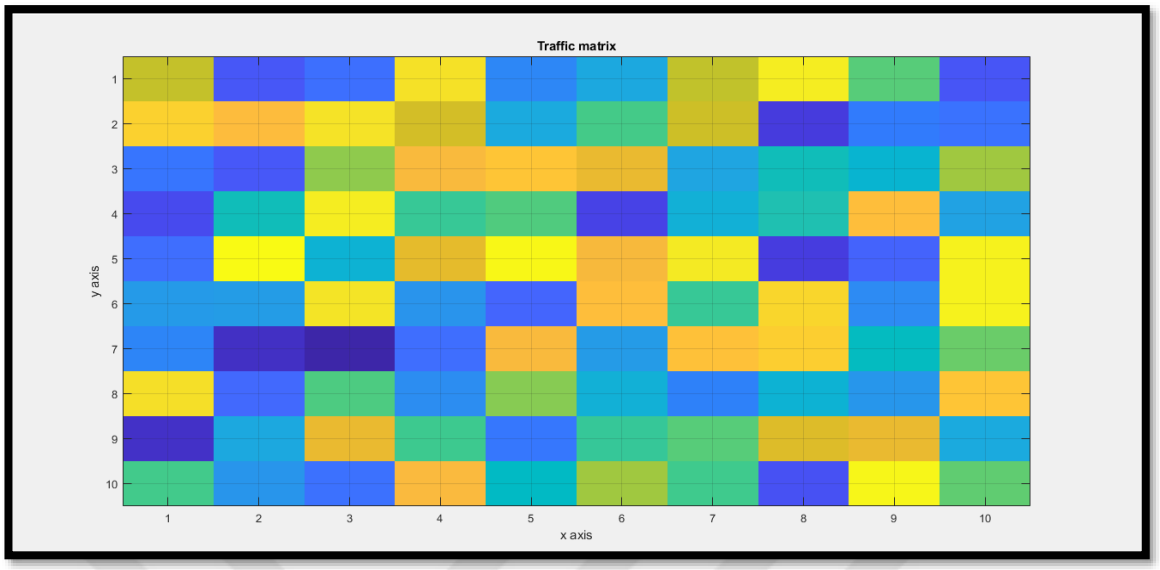

Figure 4.4: Traffic Matrix

A shortest path matrix is a tool used in network analysis to identify the shortest path between pairs of nodes in a network. It is typically represented as a matrix, where each entry represents the length or cost of the shortest path between two nodes in the network.

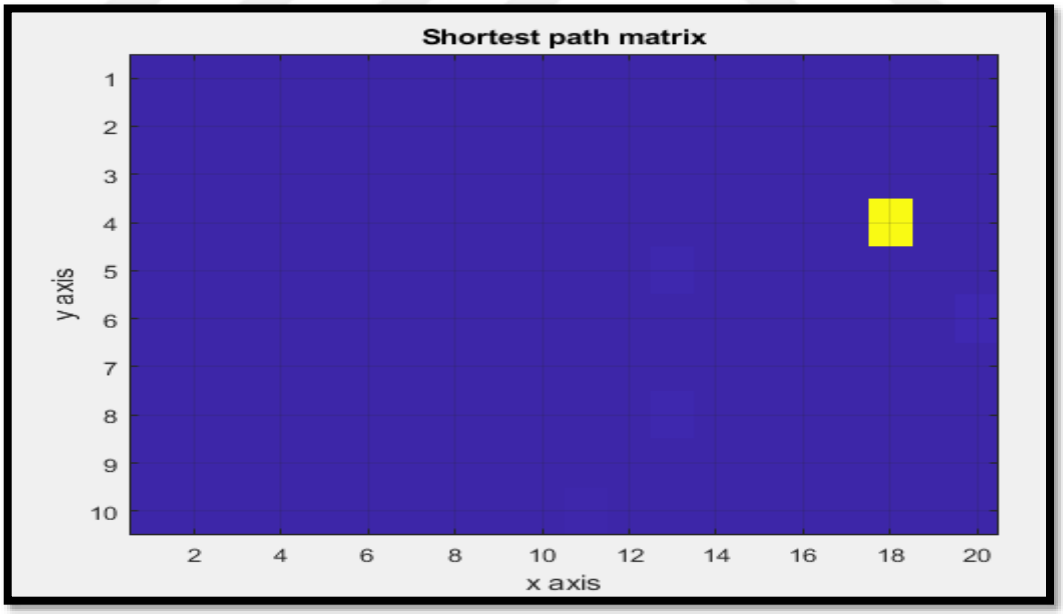

Figure 4.5: Shortest Path Matrix

A shortest path matrix is a tool used in network analysis to identify the shortest path between pairs of nodes in a network. It is typically represented as a matrix, where each entry represents the length or cost of the shortest path between two nodes in the network.

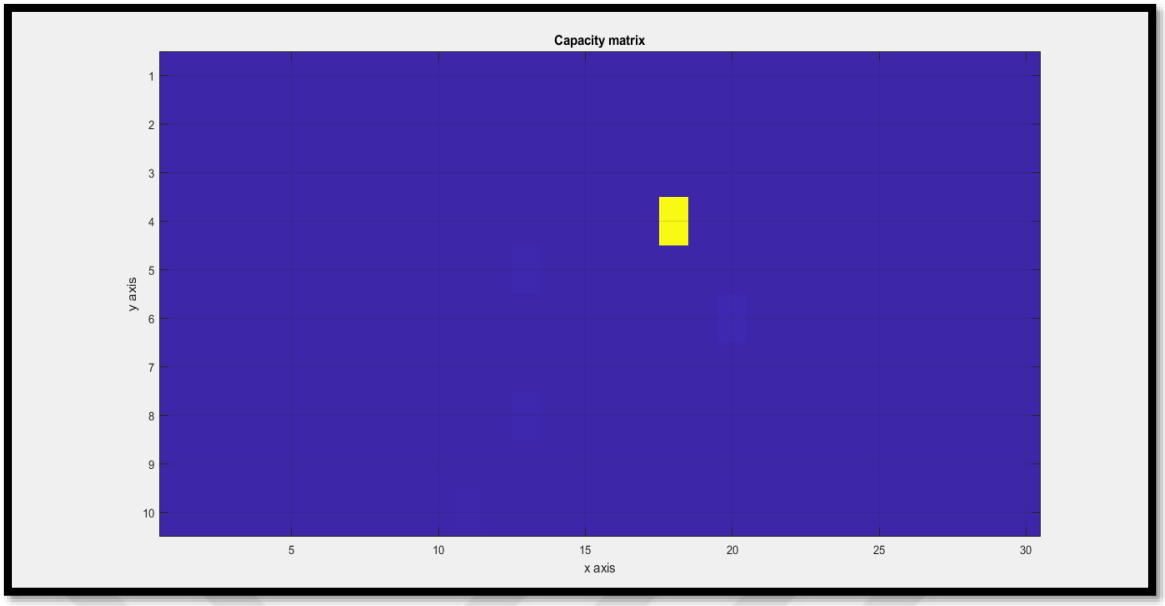

Figure 4.6: Capacity Matrix

A capacity matrix is a tool used in network planning and analysis to estimate the maximum capacity or bandwidth of the links between different nodes or devices in a network. It is typically represented as a matrix, where each entry represents the maximum capacity or bandwidth of the link between two devices in the network.

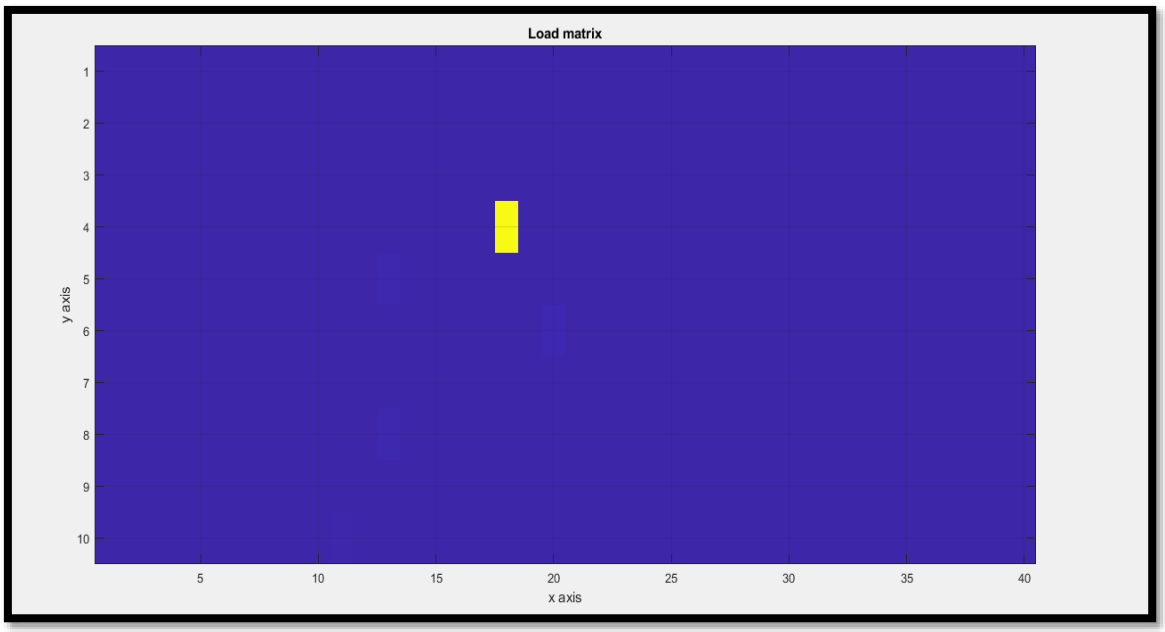

Figure 4.7: Load Matrix

A packet loss matrix is a tool used in network analysis to quantify and visualize the packet

loss rate on different links or paths in a network. It is typically represented as a matrix, where each entry represents the percentage of packets lost on a specific link or path in the network.

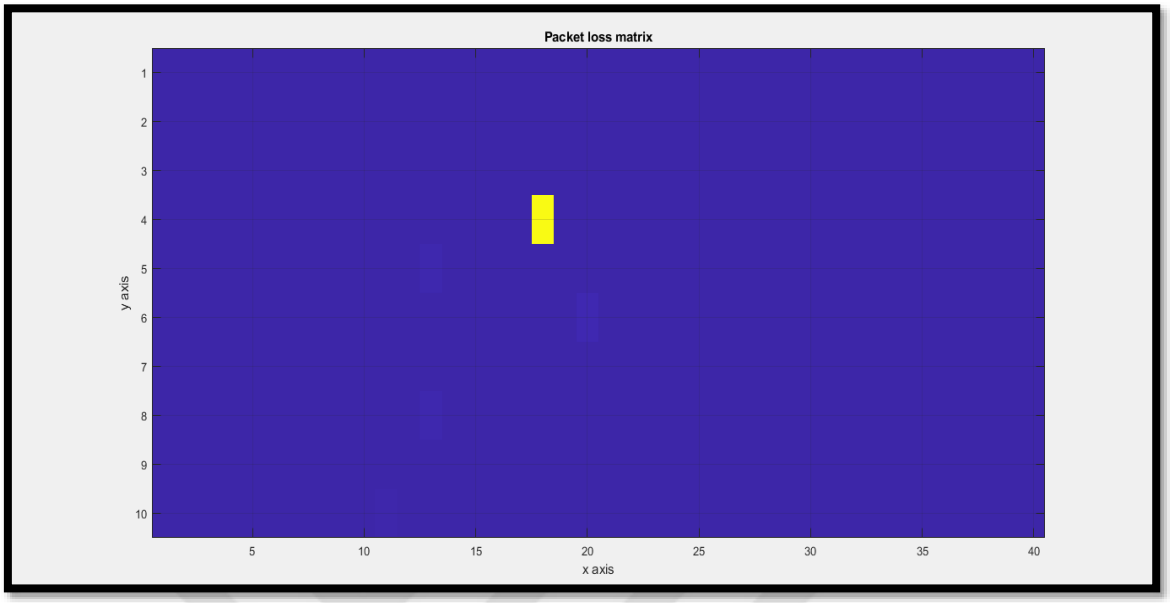

Figure 4.8: Packet Loss Matrix

Histogram of shortest paths is a graphical representation of the frequency distribution of shortest paths in a network. It shows the number of nodes or pairs of nodes that have a certain shortest path length.

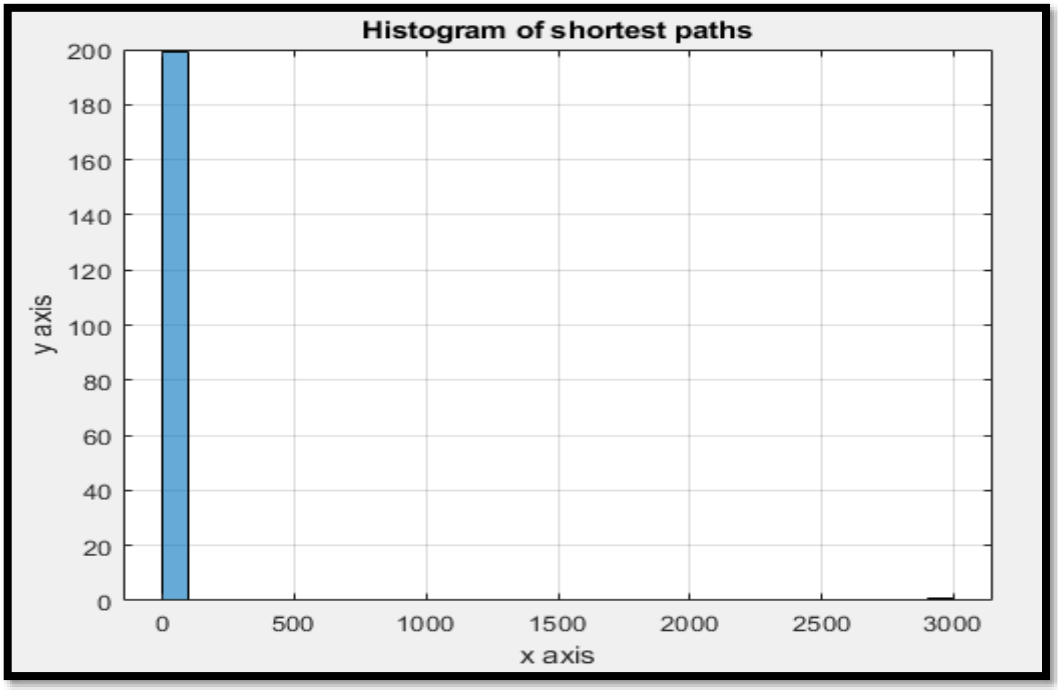

Figure 4.9: Histogram of Shortest Path

A histogram of capacities is a graphical representation of the frequency distribution of link capacities in a network. It shows the number of links that have a certain capacity range.

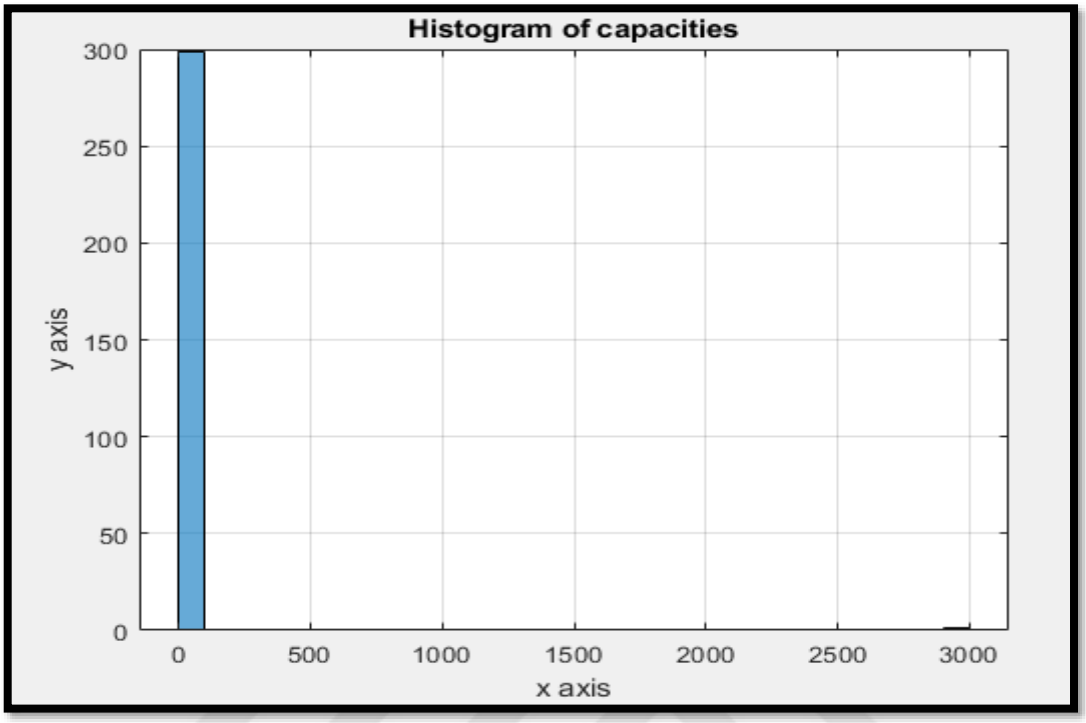

Figure 4.10: Histogram Of Capacities

A histogram of packet losses is a graphical representation of the frequency distribution of packet loss rates in a network. It shows the number of packets that have been lost within a certain packet loss rate range.

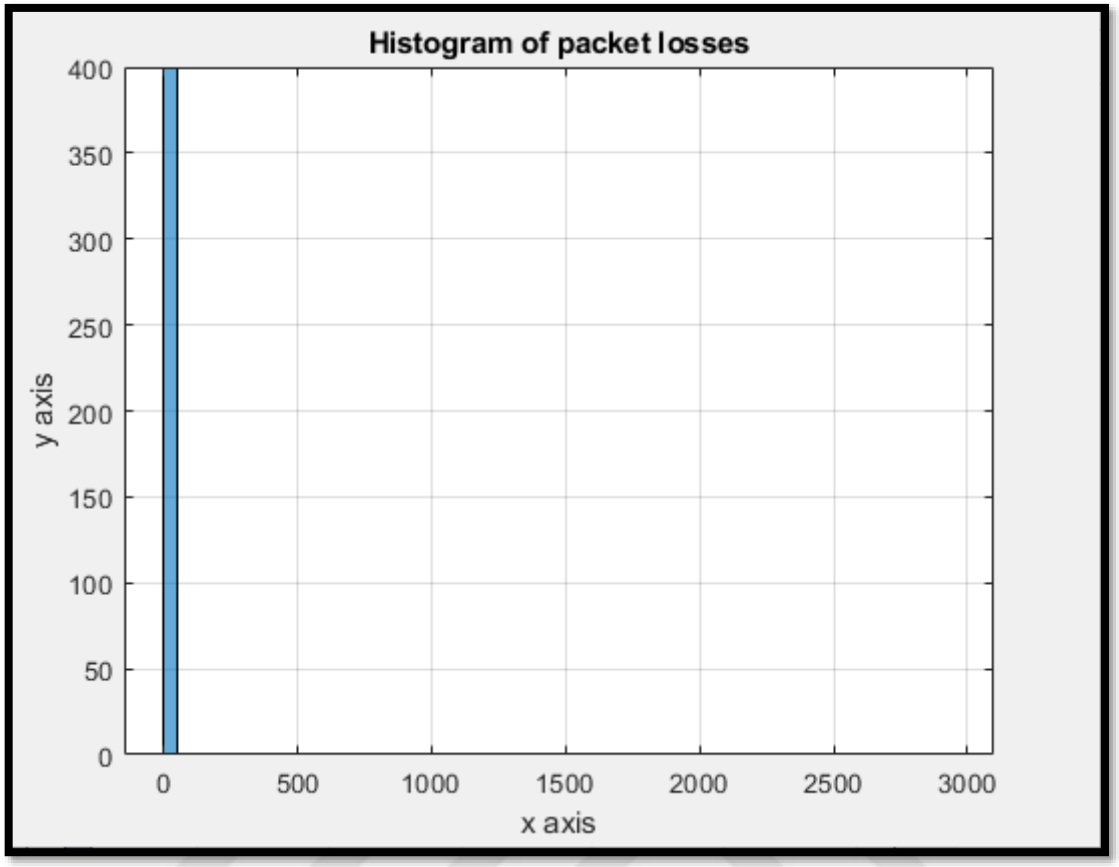

Figure 4.11: Histogram of Packet Losses

Towards the conclusion of this chapter, the model and results of intrusion detection utilizing two distinct data sets will be given. The initial batch, which was assembled in June 2016, comprised of six distinct invasions that were each tested sequentially. The second batch, which consists of eight independently tested intrusions, was compiled in March 2017. Using the WLAN experiment, several data sets were gathered throughout this cyber-security examination. Owing to the likelihood that the majority of these data sets reflect the same types of invasions with varying option selections, we have opted to just present the results for the first two data sets. The second section introduces strategies for the grouping of variables and signal processing of selected telemetry sources. Before they could be utilized to create a model, these signals had to be preprocessed because they all increased monotonically. These are the sample results from June and March. The results for each set include intrusion attempts, correlation coefficient plots for each group of variables, and SPRT plots for two selected signals from each model. Using the provided approaches, it is evident that all explored intrusions can be identified in at least one model based on these

findings. This section concludes with a summary of all intrusion classes analyzed in this study, as well as a list of the numerous intrusion testing tools and exploit programs. The key subjects of discussion will be the objectives of each type of intrusion, their implementation, and the elements that permitted or prevented the discovery of a particular intrusion during testing. Below is a qualitative evaluation of the supplied intrusion detection system.

Table 4.2: General Comparison Between Several Existing System With Our Proposed Architecture.

ARTICLE	METHOD	ACCURACY
[64]	Supervised Ensemble Learning (SEL)	84.13%
[65]	Support Vector Machine (SVM)	92.73%
Proposed	WLAN	97.86%

5. CONCLUSION

The goal of studying Wireless LAN Design and Future Internet Architecture is to develop a better understanding of the technologies that are shaping the way in which we communicate and interact with the digital world. This can be accomplished by gaining a deeper familiarity with the subject matter. These subjects are being researched because: Wireless local area networks (also known as WLANs) and fixed wireless access (also known as FIA) are both necessary parts of the modern communication systems that are in use today. The advancement of either of these fields has the potential to have a significant impact on the ways in which we work, learn, and communicate with one another.

i. The primary objective of research into WLAN design is to develop wireless networks that are not only efficient and effective, but also provide users with connectivity that is dependable and secure. This goal is the primary motivation behind the research. In order to satisfy the ever-increasing demand for wireless communication, the implementation of WLANs has become an absolute requirement. The ever-increasing demand for portable electronic gadgets like smartphones, tablets, and laptops is primarily responsible for this phenomenon. WLANs are also widely used in business settings because they provide the flexibility and mobility that is required for modern work practices. This is one of the main reasons why WLANs are so popular in business environments. Additionally, WLANs are seeing widespread adoption in residential settings.

ii. The production of wireless local area networks (WLAN) that are optimized for the specific conditions of the environment in which they are deployed is the objective of the design process for WLANs. Because of this, it is necessary to consider a number of different factors, some of which are interference, coverage, bandwidth, and security. WLAN designers can create networks that minimize interference and other performance issues while still providing the necessary coverage, bandwidth, and security because they understand these factors and use appropriate wireless standards and frequency bands.

iii. Improving the dependability and performance of wireless networks is another objective that can be accomplished through the study of WLAN design. This is one of the many benefits of studying WLAN design. As a result of this, the development of new technologies and methods that can improve the performance of networks, reducing the amount of interference they experience, and providing more flexibility and scalability is required. Research in this field is primarily focused on the creation of innovative antenna technologies, signal processing algorithms, and network management tools that can assist in improving the efficiency of WLANs.

iv. The research that is currently being done on the future architecture of the internet has as its primary objective the development of an internet infrastructure that is more scalable, secure, and flexible for it to be able to meet the demands of contemporary communication systems. The current TCP/IP infrastructure is becoming less and less utilized as time goes on, and it is unable to keep up with the ever-increasing demand for bandwidth and connectivity. A researcher presents new ideas for technologies and architectures that, if implemented, could produce an internet infrastructure that is both more robust and reliable. These new ideas are presented as part of the researcher's presentation.

v. The study of FIA has many goals, one of the most important of which is to develop network architectures that are more efficient and flexible and that can support the rising demand for bandwidth and connectivity. Among the many goals that the study of FIA aims to achieve, one of the most important of these is to develop FIA. This includes the utilization of technologies such as SDN and NFV, which can make it possible for network administrators to control and manage networks in a manner that is more effective and efficient. Specifically, this refers to the SDN and NFV technologies. In addition to this, the researcher is working on the development of new routing protocols, network topologies, and other technologies that have the potential to provide increased scalability as well as reliability.

vi. Another one of the goals of FIA research is to protect the privacy of internet users while simultaneously enhancing the safety of those who use the internet. The rate at which increasingly complex digital technologies are being adopted coincides with a

corresponding increase in the likelihood of cyberattacks and data breaches. New security architectures and protocols have been proposed by the Financial Industry Regulatory Authority (FIA), which have the potential to protect the data and privacy of users, as well as prevent unauthorized access and data breaches. The work that is being done in this area of research includes the creation of advanced encryption and authentication protocols, intrusion detection and prevention systems, and various other security technologies.

vii. Students can acquire a deeper comprehension of the technologies that are influencing the development of contemporary communication systems by studying topics such as wireless LAN design and future internet architecture. In a nutshell, this will help students acquire a more well-rounded understanding of the technologies. By improving the dependability, security, and performance of wireless networks as well as the infrastructure of the internet, researchers have the potential to transform the digital world into a place that is both better connected and more productive. This will make it possible for the digital world to support the requirements of both businesses and individuals, as well as the requirements of society.

viii. In conclusion, WLAN design and future internet architecture are rapidly evolving areas of research, and their implementation on MATLAB can provide numerous benefits. By using MATLAB to model and simulate WLANs and future, internet architectures, researchers can evaluate the performance of different design choices and protocols, as well as develop and test new algorithms and protocols. These advancements can lead to the development of more efficient, reliable, and secure networks that can meet the growing demands of the digital age. Therefore, the use of MATLAB in WLAN. design and future internet architecture implementation can greatly contribute to the advancement of networking technology, and drive innovation in the field for years to come.

5.1 FUTURE RECOMMENDATIONS

This paper's behavior-based detection algorithms were good at detecting several incursion behaviors, although this study might be expanded in various ways. The virtual WLAN testing environment simulates certain assumptions. Many industrial processes and WLAN server dynamics are periodic. A large NPP or cyber-physical system with hundreds or thousands of sensors was expected to create a lot of network traffic. Many assumptions were made to collect relevant data from a working WLAN or mission-critical corporate network. After cleaning, genuine system telemetry may improve simulation accuracy. If so, the simulation could be changed to better depict the system's signal dynamics. The evaluation could simulate WLAN system processes without actual data. The test bed servers may build and operate a small flow loop with sensing and control components. The principal test bed server (including the WLAN server) can periodically poll sensors, give commands, and collect data. The test environment's extra servers could become flow loop management and monitoring RTUs. If not, the test bed's servers could run a commercial NPP simulator. Penetration testing could remotely attack a portion of the new system's components to find those vulnerable to the methods below. These methods boost data-driven model process telemetry. In conclusion, the given methods failed to find many previously tested and well-implemented vulnerabilities. The system's dynamics don't explain for many of these attacks' speed. These exploits are often overlooked during data collection due to their short execution time. Additional audit documentation that proves these assaults may work. It could be used with behavioral techniques to create a knowledge-based detection system.

REFERENCES

[1] Yankson, B., Loucks, T., Sampson, A., & Lojano, C. (2023, February). Robots Security Assessment and Analysis Using Open-Source Tools. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 449-456). http://dx.doi.org/10.34190/iccws.18.1.1019

[2] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436.

[3] Kovacich, G. L., & Jones, A. (2002). What InfoSec professionals should know about information warfare tactics by terrorists. Computers & Security, 21(1), 35-35. https://doi.org/10.54675/STTN2091

[4] Anderson, J. P. (1980). Computer security threat monitoring and surveillance. Technical Report, James P. Anderson Company.

[5] Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR), 46(4), 1-29. https://doi.org/10.1145/2542049

[6] Ou, Y. J., Lin, Y., & Zhang, Y. (2010, April). The design and implementation of host-based intrusion detection system. In 2010 third international symposium on intelligent information technology and security informatics (pp. 595-598). IEEE. https://doi.org/10.1109/IITSI.2010.127

[7] Ni, L., & Zheng, H. Y. (2007, August). An unsupervised intrusion detection method combined clustering with chaos simulated annealing. In 2007 International Conference on Machine Learning and Cybernetics (Vol. 6, pp. 3217-3222). IEEE. https://doi.org/10.1155/2022/8714870

[8] Ahmed, A., Razak, S., Hanan, A., & Osman, I. (2012). Detection Techniques in MANET. In Proceedings of the International Conference on Wireless Networks (ICWN) (p.

1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied

Computing (WorldComp). https://link.springer.com/chapter/10.1007/3-540-45474-8_11#:~:text=DOI%3A%2010.1007/3%2D540%2D45474%2D8_11

[9] Gao, W., Morris, T., Reaves, B., & Richey, D. (2010, October). On WLAN control system command and response injection and intrusion detection. In 2010 eCrime Researchers Summit (pp. 1-9). IEEE.

[10] Gong, Y., Mabu, S., Chen, C., Wang, Y., & Hirasawa, K. (2009, August). Intrusion detection system combining misuse detection and anomaly detection using genetic network programming. In 2009 ICCAS-SICE (pp. 3463-3467). IEEE.

[11] Luo, Y. X. (2010, May). The research of Bayesian classifier algorithms in intrusion detection system. In 2010 International Conference on E-Business and E-Government (pp. 2174-2178). IEEE.

[12] Hines, J.W., Yang, D. and Usynin, A., "WLAN System Monitoring and Diagnostics Using Empirical Models", Final Report, Battelle Energy Contract # 00050837, September 2007.

[13] Boyer, S., "WLAN – Supervisory Control and Data Acquisition 3rd Edition", ISA, 2004.

[14] Cazorla, L., Alcaraz, C., & Lopez, J. (2013). Towards automatic critical infrastructure protection through machine learning. In Critical Information Infrastructures Security: 8th International Workshop, CRITIS 2013, Amsterdam, The Netherlands, September 16-18, 2013, Revised Selected Papers 8 (pp. 197-203). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-03964-0_18#:~:text=DOI%3A%2010.1007/978%2D3%2D319%2D03964%2D0_18

[15] Ahmed, I., Obermeier, S., Naedele, M. and Richard III, G.G., "WLAN systems: Challenges for forensic investigations", Computer, 2012.

[16] Jain, P., & Tripathi, P. (2013). WLAN security: a review and enhancement for DNP3 based systems. CSI transactions on ICT, 1, 301-308.

[17] Han, S., Xie, M., Chen, H. H., & Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. IEEE systems journal, 8(4), 1052-1062. https://doi.org/10.1109/JSYST.2014.2373851

[18] Penetration Testing Tools (PTT), 2016, http://www.pen- tests.com/difference-between-threat-vulnerability-and-risk.html.

[19] Dressler, F., "Self-Organization in Autonomous Sensor and Actuator Networks", New York, NY, USA: Wiley, 2007.

[20] Neuman, C., "Challenges in security for cyber-physical systems", Proc. DHS Workshop Future Directions Cyber-Phys. Syst. Security, Newark, NJ, USA, July, 2009.

[21] Zhu, B., Joseph, A. and Sastry, S., "A taxonomy of cyber-wireless network attacks on WLAN systems", IEEE International Conference on Cyber, Physical and Social Computing, Dalian, China, Oct. 2011.

[22] Tsang, R., "Cyberthreats, Vulnerabilities and wireless network attacks on WLAN Networks", University of California, Berkeley, 2010.

[23] Fovino, A., Coletta, A. and Masera, A., "Taxonomy of security solutions for the WLAN sector", 2010.

[24] Makhija, J., & Subramanyan, L. (2003). Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus. Electronics Systems Group, IIT Bombay, India, Tech. Rep.

[25] Beresford, D., January, 2011, http://thesauceofutterpwnage.blogspot.com.

[26] Shao, Z., Zhuge, Q., He, Y., & Sha, E. M. (2003, December). Defending embedded systems against buffer overflow via hardware/software. In 19th Annual Computer Security

Applications Conference, 2003. Proceedings. (pp. 352-361). IEEE. https://doi.org/10.1145/3538275

[27] Paukatong, T. (2005, August). WLAN security: A new concerning issue of an in-house EGAT- WLAN. In 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific (pp. 1-5). IEEE.

[28] CleveWLANd, D., "IEC TC57 security standards for the power systems info infrastructure: beyond simple encryption", 2005.

[29] Kleinman, A., & Wool, A. (2014). Accurate modeling of the siemens s7 scada protocol for intrusion detection and digital forensics. The Journal of Digital Forensics, Security and Law: JDFSL, 9(2), 37.

[30] Almalawi, A., Yu, X., Tari, Z., Fahad, A., & Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Computers & Security, 46, 94-110. https://doi.org/10.1016/j.cose.2014.07.005

[31] Baker, S. A., Filipiak, N., & Timlin, K. (2011). In the dark: Crucial industries confront cyber attacks. McAfee, Incorporated.

[32] ICS-CERT 2013, ICS-CERT Monitor Report between April-June 2013. Department of HomeWLANd Security, June 17, 2013.

[33] Bailey, M., Cooke, E., Jahanian, F., & Watson, D. (2005). The blaster worm: Then and now. IEEE Security & privacy, 3(4), 26-31. https://doi.org/10.1109/MSP.2005.106

[34] Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[35] Cheminod, M., Durante, L., & Valenzano, A. (2012). Review of security issues in industrial networks. IEEE transactions on industrial informatics, 9(1), 277-293. https://doi.org/10.1109/TII.2012.2198666

[36] Luzwick, P. (2001). Businesses Can Profit from Information Warfare Tactics. Computer Fraud & Security, 2001(5), 16-17. https://doi.org/10.1016/S1361-3723(01)00518-8

[37] Markey, E. (2003). Infection of the Davis Bessie Power Plant by the. Slammer" Worm Computer Virus–Follow-up Questions.

[38] Abrams, M., & Weiss, J. (2007). Bellingham, Washington, control system cyber security case study. National Institute of Standards and Technology (NIST). Recuperado de http://csrc. nist. gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report, 202.

[39] Parfomak, P. W. (2012, August). Pipeline cybersecurity: Federal policy. Congressional Research Service, Library of Congress.

[40] Slay, J., & Miller, M. (2008). Lessons learned from the maroochy water breach (pp. 73-82). Springer US.

[41] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436. https://doi.org/10.1016/j.cose.2012.02.009

[42] Dacey, R. F. (2004). Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. US General Accounting Office.

[43] Jeffries, B., Hines, J. W., & Gross, K. C. (2017, June). Behavior-based approach to misuse detection of a simulated SCADA system. In Proc. 10th Nucl. Plant Instrum. Control Hum., Mach. Interface Technol. (pp. 1761-1771).

[44] Vinchurkar, D. P., & Reshamwala, A. (2012). A review of intrusion detection system using neural network and machine learning. J. Eng. Sci. Innov. Technol, 1, 54-63.

[45] Jyothsna, V. V. R. P. V., Prasad, R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. International Journal of Computer Applications, 28(7), 26-35.

[46] Park, K., Lin, Y., Metsis, V., Le, Z., & Makedon, F. (2010, June). Abnormal human behavioral pattern detection in assisted living environments. In Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments (pp. 1-8).

[47] Carcano, L., "A multidimensional critical state analysis for detecting intrusions in WLAN systems", IEEE Transactions on Industrial Informatics, Vol. 7, No. 2, May 2011.

[48] Lauf, A. P., Peters, R. A., & Robinson, W. H. (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Networks, 8(3), 253-266. https://doi.org/10.1016/j.adhoc.2009.08.002

[49] Killourhy, K. S., & Maxion, R. A. (2009, June). Comparing anomaly-detection algorithms for keystroke dynamics. In 2009 IEEE/IFIP International Conference on Dependable Systems & Networks (pp. 125-134). IEEE. https://doi.org/10.1109/DSN.2009.5270346

[50] Shin, S., Kwon, T., Jo, G. Y., Park, Y., & Rhy, H. (2010). An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. IEEE Transactions on Industrial Informatics, 6(4), 744-757. https://doi.org/10.1109/TII.2010.2051556

[51] Garitano, I., Uribeetxeberria, R. and Zurutuza, U., "A Review of WLAN Anomaly Detection", Electronics and Computing Department, Mondragon University, 2011.

[52] Tsang, R., "Cyberthreats, Vulnerabilities and wireless network attacks on WLAN Networks", University of California, Berkeley, 2010.

[53] Zimmer, C., Bhat, B., Mueller, F., & Mohan, S. (2010, April). Time-based intrusion detection in cyber-physical systems. In Proceedings of the 1st ACM/IEEE International

Conference on Cyber-Physical Systems (pp. 109-118). https://doi.org/10.1145/1795194.1795210

[54] Vigna, G., & Kruegel, C. (2006). Host-based intrusion detection. na.

[55] Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, T., Ho, C., ... & Mansur, D. (1991, October). DIDS (Distributed Intrusion Detection System)–Motivation. In Architecture, and an Early Prototype, InProceedings of the 14th National Computer Security Conference, Washington, DC (pp. 167-176).

[56] Sabri, F. N. M., Norwawi, N. M., & Seman, K. (2011). Identifying false alarm rates for intrusion detection system with data mining. IJCSNS: International Journal of Computer Science and Network Security, 11(4), 95-99.

[57] Ho, C. Y., Lin, Y. D., Lai, Y. C., Chen, I. W., Wang, F. Y., & Tai, W. H. (2012). False positives and negatives from real traffic with intrusion detection/prevention systems. International Journal of Future Computer and Communication, 1(2), 87.

[58] Han, H., Lu, X. L., & Ren, L. Y. (2002, November). Using data mining to discover signatures in network-based intrusion detection. In Proceedings. International Conference on Machine Learning and Cybernetics (Vol. 1, pp. 13-17). IEEE. https://doi.org/10.1109/ICMLC.2002.1176698

[59] Ou, Y. J., Lin, Y., & Zhang, Y. (2010, April). The design and implementation of host-based intrusion detection system. In 2010 third international symposium on intelligent information technology and security informatics (pp. 595-598). IEEE. https://doi.org/10.1109/IITSI.2010.127

[60] Haddadi, F., & Sarram, M. A. (2010, April). Wireless intrusion detection system using a lightweight agent. In 2010 Second International Conference on Computer and Network Technology (pp. 84-87). IEEE. https://doi.org/10.1109/ICCNT.2010.26

[61] White, G. B., Fisch, E. A., & Pooch, U. W. (1996). Cooperating security managers: A peer-based intrusion detection system. IEEE network, 10(1), 20-23. https://doi.org/10.1109/65.484228

[62] Whitman, M. E., & Mattord, H. J. (2021). Principles of information security. Cengage learning.

[63] Hinton, G., & Sejnowski, T. J. (Eds.). (1999). Unsupervised learning: foundations of neural computation. MIT press.

[64] Tran, T. P., Tsai, P., Jan, T., & He, X. (2012). Machine Learning Techniques for Network Intrusion Detection. In Machine Learning: Concepts, Methodologies, Tools and Applications (pp. 498-521). IGI Global. https://www.igi-global.com/chapter/machine-learning-concepts-methodologies-tools/56160#:~:text=DOI%3A%2010.4018/978%2D1%2D60960%2D818%2D7.ch310

[65] Alsubaie, F., Al-Akhras, M., & Alzahrani, H. A. (2020, November). Using machine learning for intrusion detection system in wireless body area network. In 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) (pp. 100-104). IEEE. https://doi.org/10.1109/SMART-TECH49988.2020.00036