Journal of Modern Technology and Engineering
Vol.10, No.1, 2025, pp.5-25
https://doi.org/10.62476/jmte.10105

Jomard Publishing

ENHANCING WIRELESS SECURITY THROUGH DEEP LEARNING: NETWORK ATTACK DETECTION AND ADVANCED CLASSIFICATION

Noor Raad Saadallah[1], **Salah Abdulghani Alabady**[2*], **Neam Tariq Hussin Almalah**[1]

[1]Computer and Information Engineering Department, College of Electronics Engineering, Ninevah University, Mosul, Iraq
[2]College of Engineering, Computer Engineering Department, University of Mosul, Iraq

Abstract. This paper delves into the realm of enhancing wireless security through the application of deep learning techniques for network attack detection and advanced classification. By leveraging the power of machine learning algorithms, particularly deep neural networks, the study aims to address the evolving challenges of securing wireless networks. The research explores the utilization of generative adversarial networks to generate synthetic features for analyzing Wi-Fi signal quality, as well as the development of hybrid security analysis systems combining model-checking techniques and deep learning for malware detection in IoT applications. Furthermore, the paper investigates the effectiveness of deep learning models in predicting cyber-attacks and detecting network intrusions, emphasizing the importance of combining traditional machine learning approaches with deep learning for improved classification of network attacks. Through a comprehensive review of existing literature and research directions, the study highlights the potential of deep learning for fortifying wireless security and offers insights into future advancements in this critical domain.

Keywords: Wireless Security, Deep learning, Network attack detection, IoT security, Advanced classification, Malware detection, Cyber-attack prediction.
AMS Subject Classification: 68M15.
Corresponding author: Salah A. Alabady, College of Engineering, Computer Engineering Department, University of Mosul, Iraq, e-mail: *eng.salah@uomosul.edu.iq*
Received: 12 September 2024; Revised: 3 January 2025; Accepted: 4 February 2025; Published: 30 April 2025.

1 Introduction

The increasing vitality of real-time and verifiable intelligence on the security of networks led to the development of new machine learning (ML) techniques for the elaborated analysis and modeling of network measurements based on artificial intelligence (AI) for improved network security. The premonitory alarm before any unfavorable occurrence is sought by the AI in a way that can identify the non-correlated security data, recognize the commonalities among the data, and falsify any deviating ones. Especially supervised and unsupervised ML is a popular tool and model used in AI-based network intrusion detection systems. The existing techniques mainly exploit ML and deep learning (DL) techniques for wireless network (WN) security, including clustering-based techniques for WN attack detection, signature matching for WN security, anomaly detection models for WN security, and classification models for WN security.

The study of different types of attacks and their detection is an important area of wireless communication. These attacks can be categorized into signaling manipulation, routing attacks,

spectrum attacks, jamming attacks, hardware impairment attacks, denial-of-service (DoS), physical layer, energy depletion, browser-based, and cross-site scripting (XSS) attacks (Javeed et al., 2021). They all affect the performance of the network. Finding out the type of attack and its impacts has been a challenging issue in wireless communication. Researchers are still looking for complete solutions for the attack detection and classification problems. Many mitigation and avoidance techniques have been proposed in the literature to address the wireless attacks performed in the network (Ahmad et al., 2022a). The available solutions generally incorporate three types of systems: monitoring systems, signature systems, and anomaly detection systems. All the approaches have their own merits and demerits. Signature-based systems can catch known attacks; on the other hand, the anomaly detection system can catch unknown attacks. The desired features will be perfect coordination among these systems, but it is still not a complete solution (Tandiya et al., 2018a). Anomaly detection systems (ADSs) based on ML and DL have been widely tested in wired networks. However, there are challenges to applying these models directly to a wireless environment (Wazirali et al., 2021). With the development of deep learning, the robustness and accuracy of the ADS have been significantly improved, enabling it to be directly applied to the wireless environment. Generative adversarial networks are exploited to create synthetic features based on received signal strength indicators (RSSI) in Wi-Fi signal strength diagrams. Deep autoencoders and convolutional neural networks have been used to classify users based on wireless devices' time and space models in wireless networks. Deep learning models have proven to be effective in classifying user actions, interference and web activity, thus making them suitable for use in wireless web attack detection.

Wireless networks have become increasingly popular because of their lower installation security requirements, cost-effectiveness, and minimal infrastructure needs. Nonetheless, the inherent openness of wireless networks renders them more vulnerable to assaults (Castelli et al., 2021). A significant quantity of wireless fidelity (Wi-Fi) and Internet of Things (IoT) devices have been documented as susceptible to various assaults. Traditional measures, such as firewalls and encryption techniques, are insufficient for safeguarding wireless networks (Hamza et al., 2022). Therefore, it is essential to create innovative, precise, and sophisticated solutions for ongoing surveillance and alarm production in the event of network intrusions. This publication presents the following contributions:

1. Requirement of Deep Learning in Wireless Security: The paper delves into the use of deep learning techniques, such as convolutional neural networks and generative adversary networks, to enhance wireless security through network attack detection and a detailed paragraph 3. (Deep Learning Models for Wireless Security).

2. New methods for malware detection: The study presents a hybrid security analytics framework that combines model testing techniques and deep learning for better malware detection in IoT applications and cyber security in connected devices - addresses growing concerns about threats.

3. Advanced cyber-attack prediction: Advanced cyber-attack prediction: Through the use of deep learning models, the paper contributes to the enhancement of cyber-attack prediction capabilities to identify networks.

4. Better classification of network attacks: The study demonstrates the effectiveness of combining traditional machine learning techniques with deep learning to create advanced network attack classification, resulting in more robust security measures combating the growing threat of cyber threats.

This paper provides a comprehensive introduction to wireless security and deep learning. The paper is organized as follows: An overview of wireless security is given in Section 1, with a thorough discussion of the advances in wireless networks, followed by an overview of Wi-Fi security threats. Section 2 gives an overview of deep learning with various architectures and

types of methods. Section 3 provides an in-depth technical review of deep learning models for both network attack detection and classification. That section also covers recent advancements and challenges in the deployment of deep learning. Section 4 concludes this paper.

1.1 Overview of Wireless Security Threats

Threats and weaknesses can be addressed by the encryption of data transmitted by the link layer protocol and by limiting the physical layer to permit connection for only brief intervals. Additional security services can be obtained through the wireless network protocol by employing either traditional security protocols or the dual protocols of WPA and WPA2. Although companies have upgraded their wireless devices to the WPA3 protocol to address some security vulnerabilities of earlier versions, WPA3 itself possesses significant deficiencies in its foundational security frameworks. The security services at the physical and link layers can offer a degree of wireless protection; however, current wireless security is limited in its capacity to detect adversary actions that may target higher-level protocols. New standards for wireless systems are being standardized to provide security services to upper layer protocols. Intelligence-based attack detection in wireless networks can be achieved through (a) manual definition of security parameters by network operators or (b) automatic detection of assaults without human interaction. Automated attack detection systems exhibit more dependability than those employing manual security setups. Network-based attack detection approaches heavily depend on intricate factors, such as observed network traffic flows. The second kind of attack detection system is host-based, which analyzes information from packet payloads or other physical layer components to identify the sort of network assault using specialized cognitive models. The threats targeting wireless networks can be executed on various layers of communication. At the physical layer, an attacker can transmit a jamming signal to the targeted wireless network to block or interrupt the communication network (Baishya and Manoj, 2024). The attacks that target the link layer are more complicated, as attackers have to select a network frame over the air, analyze the packet header, and decode the packet. For example, a simple denial of service can be easily executed at the link layer by broadcasting the de-authentication frames (da Silva et al., 2022). The attacks that target the link layer can also be used for the impersonation of a valid node, replay the previously encrypted messages, or eavesdrop the running communication link (Albasheer et al., 2022).

1.2 Wireless Attacks

Wireless communication has received more attention from academicians and researchers as security has become a primary concern. The reason is that while transmitting data over wireless communication, anyone can easily receive it. It is flexible as well as cost-effective when compared to wire LANs, and it provides communication that is easy to deploy. The protocols of wireless, which provide functionality like medium access control, are defenseless to cyber-attacks. The protocols, as well as the infrastructure, are based on trust; it is more prone to threats in wireless communication. They are developing fast, not just in a positive sense but also in a negative sense; they are being utilized more as a tool by hackers due to various vulnerabilities in wireless networks. Wireless communication has changed how the world communicates today (Bhatti et al., 2022). It is important to have a good understanding of the types of cyber-attacks that several wireless systems are exposed to today (Shukla et al., 2009). There are various types of wireless networks, like Mobile Ad-hoc Networks (MANET), wireless sensor networks (WSN), wireless body area networks (WBAN), ad-hoc on-demand distance vector (AODV), and wireless local area networks (WLAN) (Alam and De, 2014).

Each of the wireless networks is prone to different types of attacks due to different configuration settings of the transmission medium and networks. Some of the prevalent methods for achieving this are altering, modifying, deleting, or inserting packets to disrupt wireless com-

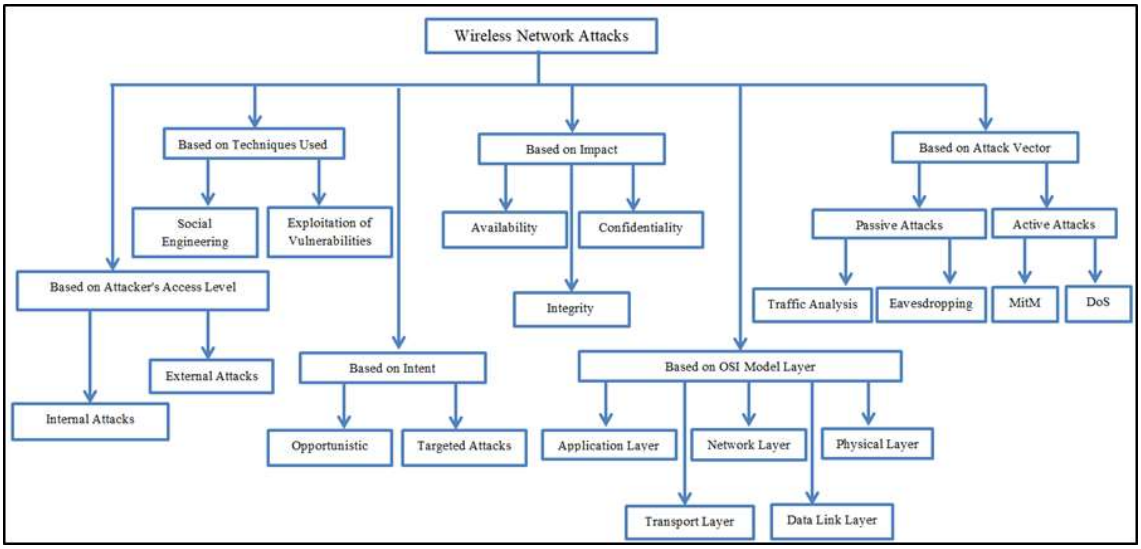

Figure 1: Types of wireless attacks

munication. Hence, techniques and methods are developed for detecting and defending against the different wireless attacks for secure communication. Certain wireless attacks occur on the wireless network running on the data-link layer and network layer, namely, jamming attacks, wormhole attacks, and black hole attacks. Such wireless attacks disrupt communication between different nodes and can ultimately stop network traffic. Here we describe the major types of wireless attacks: eavesdropping, de-authentication, and disassociation attacks. An eavesdropping attack is an unauthorized activity in which an attacker secretly intercepts and manages data over a Wi-Fi connection. This attack is most commonly deployed when a user is using an open network and providing no encrypted communication. A de-authentication attack constitutes a denial-of-service attack; an attacker initiates an assault using malicious de-authentication frames. The target is coerced and excluded from the Wi-Fi network throughout the execution of this assault. This is performed to sever a user's connectivity and transition the user to mesh mode. The victim, who should be connected to the network, receives the suspiciously constructed frames from an attacker. Disassociation is an assault akin to the de-authentication attack. Figure 1 and Table 1 shows types of wireless attacks.

To better understand the gravity and technical implications of these wireless attacks, it is important to analyze their computational complexity and specific conditions under which they succee1 d. Table 2 presents a summary comparison of several common wireless attacks, including its required computational effort, previous requirements for successful execution and the tools that are typically used. This tabular representation provides valuable information to evaluate the level of threat and the design of more specific defense mechanisms.

A dissociation attack occurs when an attacker transmits a disassociation request frame to sever the connection between a client and an access point. In recent years, the swift expansion of wireless networks, coupled with the advent of new technologies, has rendered them attractive research opportunities for the scientific community (Boni et al., 2020). Wireless network devices are susceptible to various unique types of attacks, undermining the minimal security features inherent to these devices Zhang et al. (2022). To guarantee the effective operation of network devices, it is essential to examine the specific types of attacks occurring at each layer of the wireless network model (Altaf et al., 2019). Currently, numerous forms of attacks are recognized as significant threats to the network layer. The majority of these attacks primarily focused on the operating systems of network devices, including DOS/DDOS attacks, MITM attacks, and eavesdropping packet retransmission attacks, among others. In the authentication layer,

the primary targeted attacks include viruses, Trojan horses, key loggers, and various forms of sniffing attacks. The previously mentioned attacks may result in unauthorized access to network devices. Table 3 presents several studies addressing wireless network attacks.

Table 1: Types of wireless attacks

Classifying Criteria	**Category/ Subcategory**	**Description / Example**	**References**
Based on attack vector	Active attacks	Dos, MitM	(Basu et al., 2020; Hindy et al., 2020; Alhoraibi et al., 2023a)
	Passive attacks	Eavesdropping, Traffic Analysis, spoofing, replay.	(da Silva et al., 2022; Ahmad et al., 2022b; Rathod et al., 2022; Podder et al., 2021)
Based on Impact	Availability	Jamming, DoS attacks.	(da Silva et al., 2022; Rathod et al., 2022; Podder et al., 2021)
	Confidentiality	Eavesdropping, traffic analysis.	(Basu et al., 2020; Hindy et al., 2020; Alhoraibi et al., 2023a)
	Integrity	Packet injection , MitM.	Ahmad et al. (2022b); Alhoraibi et al. (2023a); Rathod et al. (2022)
Based on Techniques Used	Social Engineering	Psychological manipulation to gain access	(Ahmad et al., 2022b; Hindy et al., 2020)
	Exploitation of Vulnerabilities	Exploiting software or protocol flaws	(Alhoraibi et al., 2023a; Rathod et al., 2022; Podder et al., 2021)
Based on Attacker's Access Level	Internal Attacks	Inside threads with access	(Basu et al., 2020; Alhoraibi et al., 2023a)
	External Attacks	Attacker outside the network	(da Silva et al., 2022; Ahmad et al., 2022b; Basu et al., 2020)
Based on Intent	Opportunistic	Non-targeted attacks exploiting easy access	Basu et al. (2020); Hindy et al. (2020)
	ETargeted Attacks	Aimed at specific systems or individuals	(Alhoraibi et al., 2023a; Rathod et al., 2022)
Based on OSI Model Layer	Physical Layer	Jamming, interference attacks	(Basu et al., 2020; Rathod et al., 2022; Podder et al., 2021)
	Data Link Layer	MAC spoofing, frame flooding	(Hindy et al., 2020; Alhoraibi et al., 2023a)
	Network Layer	Routing attacks, IP spoofing	(Alhoraibi et al., 2023a; Gong et al., 2024)
	Transport Layer	TCP SYN flooding, session hijacking	(Ahmad et al., 2022b; Alhoraibi et al., 2023a; Podder et al., 2021)
	Application Layer	Malware, spoofing application services	(Alhoraibi et al., 2023a; Mohan et al., 2022)

Table 2: Computational Attributes and Success Criteria of Common Wireless Attacks

Attack Type	**Complexity**	**Conditions for Success**	**Tools Commonly Used**	**Reference**
Jamming Attack	O(1) – O(n)	Proximity to target, unsophisticated interference, high signal power	SDRs, JammerPro, HackRF	(Hindy et al., 2020; Rathod et al., 2022)
De-authentication Attack	O(1)	Client must be connected to AP; attacker spoofs MAC address	Aireplay-ng, Wireshark	(Ahmad et al., 2022b; Alhoraibi et al., 2023a)
Eavesdropping	O(n)	Unencrypted channel, close physical proximity	Kismet, Wireshark	(Basu et al., 2020; Hindy et al., 2020)
Replay Attack	O(n)	Unprotected communication with session tokens	Scapy, Ettercap	(Albasheer et al., 2022; Alhoraibi et al., 2023a)
Spoofing (MAC/IP)	O(1) – O(n)	Weak device authentication; access to legitimate credentials or physical address	Macchanger, Arpspoof	(Alhoraibi et al., 2023a; Mohan et al., 2022)
Wormhole Attack	O(n log n)	At least two malicious nodes in different locations; low latency tunneling	Custom Python Scripts + Tunnel Setup	(Alam and De, 2014; Gong et al., 2024)
MITM (Man-in-the-middle)	O(n log n)	Session hijacking, unsecured routing protocols, improper encryption	Cain & Abel, Ettercap, Bettercap	(Alhoraibi et al., 2023a; Rathod et al., 2022)
DoS/DDoS Attack	$O(n^z)$	Bandwidth saturation, unpatched vulnerabilities, multiple botnet nodes	LOIC, HOIC, Botnets	(da Silva et al., 2022; Ahmad et al., 2022b; Rathod et al., 2022; Podder et al., 2021)
Energy Depletion Attack	O(n)	Sensor networks, continuous fake requests or heavy computation initiated by attacker	Custom Simulations or Repetitive Scripts	(Basu et al., 2020; Hindy et al., 2020)
Firmware Exploitation	O(1) – O(n)	Vulnerable version, local/remote firmware update support	Binwalk, Firmware Mod Kit	(Ahmad et al., 2022b; Alhoraibi et al., 2023a)

Table 3: Captures the Detailed Categorization of Wireless Network Attacks

Category	Description	References
External Threats	• **Eavesdropping**: Unauthorized listening to network communications. • **Interference**: Disruption of signal transmission. • **Illegal Access**: Unauthorized access to network resources.	(Aguiar-Pérez and Pérez-Juárez, 2023; Hindy et al., 2020; Alhoraibi et al., 2023a)
Classification by Impact/Nature	• **Deception**: Misleading network users or systems. • **Intrusion**: Unauthorized penetration into the network. • **Interference**: Disruption of normal network operations. • **Denial of Service (DoS)**: Overwhelming network resources to disrupt services.	(Ahmad et al., 2022b; Basu et al., 2020; Alhoraibi et al., 2023a; Rathod et al., 2022)
OSI Layer Classification	• **Physical Layer**: Attacks targeting the physical infrastructure of the network. • **MAC Layer**: Attacks targeting the Media Access Control layer. • **Network Layer**: Attacks targeting the routing and forwarding of data packets. • **Transport Layer**: Attacks targeting the transport of data across the network.	(Ahmad et al., 2022b; Hindy et al., 2020; Alhoraibi et al., 2023a; Rathod et al., 2022; Gong et al., 2024; Podder et al., 2021)
Previous Approaches	**Spectrum Sensing**: Identifying RF signals to defend against or launch attacks, especially in noisy and multi-path environments.	[16]
Types of Wireless Attacks	• DoS Attacks, Eavesdropping, Energy Depletion, MAC Layer Attacks • Firmware, Spoofing, Jamming, De-authentication/Disassociation • DDoS, AP Flooding, Packet Injection, Misconfiguration • Fragmentation Flooding, PMKID Attacks	(Ahmad et al., 2022b; Basu et al., 2020; Alhoraibi et al., 2023a; Rathod et al., 2022; Podder et al., 2021)
Intentional vs. Unintentional Attacks	• **Internal Attacks**: Within accessing threads • **Passive Attacks**: Eavesdropping without interrupting the network. • **Active Attacks**: Interfering with network operations (e.g., masquerade, MITM)	(Tandiya et al., 2018b; Basu et al., 2020; Hindy et al., 2020; Alhoraibi et al., 2023a; Rathod et al., 2022)
Passive Attack Types	• **Weak Passive Attacks**: Casual observation and intermittent recording • **Strong Passive Attacks**: Continuous capture and analysis	(Hindy et al., 2020)
Active Attack Types	• **Masquerade**, **Jamming** • **Unauthorized Transmission, Message Alteration**	(Alhoraibi et al., 2023a; Rathod et al., 2022)
Relation to OSI Model	• **Physical Layer**: Attacks on the physical infrastructure • **Data-link Layer**: Attacks using free tools and scripts	(Rathod et al., 2022; Podder et al., 2021)

1.3 Fundamentals of Deep Learning

The primary targets of DL with wireless security are Black-Hat Networks and cyber-physical systems. When deep learning is used for network attack detection, a multi-tier detection mechanism should be focused upon. In the first tier, investigate intruders who disperse ARP poisoning, host spreading, etc. In the second tier, we get the attacks' network-level meetings (DDoS, re-

flection flood, etc.). Furthermore, one can track intruders and assess the threats they could cause. Lastly, in the third tier/layer analyses, the analysis changes networks. A combination of DL and RF fingerprints so that user identity can be auto-retrieved is used to secure wireless communication in 5G and, further, 6G infrastructures. A solid collaborative information system in global radio roaming services should be designed on special fingerprints to enhance the RF of carrier-printed information. The omnidirectional logic network service starter should be used in the cellular wireless infrastructures as a safety lookout drone with the aim of user identification. Also, drones aimed at detecting vigorous databases where frequent cluster targets and user identities are managed and stored can be used. Relations between detection and logical recognition scoring need to be improved in such databases by a logic structure. Deep learning is one of the crucial computational methods inspired by brain functionality that has attracted the attention of the security community in recent years (Tandiya et al., 2018b). This is due to its potential to significantly enhance security without explicit human supervision in both the cyber and physical domains. DL explores multiple tiers of representation and abstraction that help understand data with better accuracy than other traditional methods, such as the rule-based methods that require human intervention to work effectively. DL can implicitly discover a wide range of intrinsic security properties of data and distinguish between normal and attack samples. In addition, it can analyze malware behavior and support the structure of dangerous code using the encoded latent space (Tandiya et al., 2018a). Thus, combining deep learning with wireless security seems more viable than other machine learning methods.

2 Wireless Network Attack Detection Techniques

Wireless network attack detection techniques, data traffic over wireless networks are increasing, making security a critical concern. IDS offers an additional layer of defense, but research on IDS combining 802.11-oriented and other network protocol features lags behind. The work aims to fill this gap by utilizing a modern dataset and conducting experiments with shallow and deep learning techniques. The proposed article compares Random Forest and Forward Neural Network classifiers trained on an AWID3-only dataset against the same classifiers trained on a combination of the AWID3 dataset and other network protocol features. Subsequently, recursive feature elimination and SHapley Additive exPlanations (SHAP) are used to investigate the relevance of the features and their importance. Features of the AWID3 dataset lead to stronger detection performance than 802.11 features in general, which also takes place when other traffic types are present. Nevertheless, combining 802.11 features with other protocol features results in improved performance. But hierarchical grouping of Vendor Information/Features-VI and other protocol features or HTTP and HTTPS resulted in reduced model complexity with limited performance loss. Moreover, interpretation suggests that the offload and association models are important for the detection of AP- and MM-DoS attacks and that the preponderance of traffic from a few typical devices suggests that this has an impact on the detection of AP-DoS. DP-DoS attack detection benefited most from features representing vendor activity (Chatzoglou et al., 2022).

Wireless communication is becoming a target for intruders as its benign applications and benefits grow. Data transmission security is crucial in wireless communications. These assaults must be detected and classified quickly and properly at all layers or each layer. System performance will suffer if an intrusion or attack is misclassified. So for flexibility, robustness, and pattern recognition. Learning is needed to categorize advanced attacks; however, a relatively minor change in physical (waveform attributes) or data attributes will classify a traditional assault as attack-like or benign. Wireless systems for control communications are increasingly attacked, yet certain assaults are ubiquitous and use various wireless systems. Physical and wireless methods make misleading ejection assaults easy and successful. Wireless assaults include jamming, signal, alarm, and operation-time attacks. Wireless protocols, including Wi-Fi,

HART, BLE, Cellular, VoIP, GSM, SCADA, etc., are used to execute attacks (Ahmad et al., 2022a).

As wireless systems get more complicated, several wireless and physical layer assaults are used to achieve their attack aims. The approaches are used to create hybrid assaults. The categorization and detection of this serious issue have received little attention in the literature. This complicated, multilevel structure presents several issues. There are no effective or robust security solutions to guard against these attacks; hence, new security paradigms are needed to solve wireless system security challenges (Gong et al., 2024). Semiwiki security is less strict and should be prioritized (Ma et al., 2016). Signals are susceptible to detection and jamming since they do not require a finder and are hard to identify due to their hewed frequency (Podder et al., 2021). Socializing wireless networks raises security issues that require sophisticated jamming attacks to function securely and efficiently. Jamming and collision acknowledgment are important for accurate information delivery. Jamming and collision honor the symptom model-based signal discriminator. Wireless communication models using the "Hidden Markov Model" (HMM) to discriminate signals with a single receiving antenna reflect the attack. Our method has been proven successful (Al-Turaiki and Altwaijry, 2021).

Combining attack data from many sources, collision and jamming attacks were examined for contemporaneity. Due to too many wireless terminals, the sender's data packet collided during the collision attack. Under severe load, the channel was free several times during transmission, reducing collisions, but jamming increased them. Finally, the test results from 115 observations demonstrate that the jamming and collision attack has occurred several times and caused substantial data buildup in the communication channel, resulting in channel unavailability. After prolonged jamming, the collision decreases or bumps. Wireless technology uses electromagnetic waves in three spectra: Radio Frequency (RF), Microwave, and Infrared. Widely utilized is radio frequency wireless transmission. Cellular, Bluetooth, ZigBee, and Wireless Local Area Networks choose it. Wireless antennas transfer electromagnetic waves (RF) through the air to the receiving antenna, which converts them to binary digits. The wireless technique uses 'advantage cutting' to terminate information into binary. After modulation and multiplexing, an encoding mechanism is used. These terms are shortened and discussed in certain ways. New gadgets enhance wireless network data dissipation and disruption, which may compromise wireless network security (Belarbi et al., 2022).

2.1 Traditional Methods vs. Deep Learning Approach

Initially, it is essential to implement, uphold, and adjust to the laws about biases and effort; disregard the significant variation! "A second issue is the disadvantage of tactical flexibility." When a misuser activates a detecting mechanism during the exchange of a predetermined policy, they can easily alter their attacks to evade detection. Deep learning approaches are prevalent and extensively employed for the detection of network attacks, diverging from traditional supervisory control systems. A primary contention is that deep learning architecture-particularly neural networks and contemporary learning models are compromised by advancements in computing and data processing. Upon recognizing the new dimensions of resources, the machine and gadget accessories that will determine these dimensions, the proliferation of variable sets to function as inputs, and the representation of divergent features have been identified. Nevertheless, none of the reported machine learning models to far have yielded exceptionally effective outcomes. A definition-based paradigm traditionally facilitates attack detection through pattern analysis. However, there are certain limitations due to dependence on the properties defined and derived from network data flow. In addition to this, traditional approaches require human experts to modify and maintain the updating model, as well as to develop and implement various decision rules.

Passive and active assault approaches are the two distinct categories of attacking. Passive attacks are undetectable because they do not disrupt network operations and entail the unautho-

rized observation of networks. Conversely, active network attacks have the potential to disrupt or damage a network, alter data streams, and capture or obliterate information (Tandiya et al., 2018b). The initial step in preventing these attacks is to identify the network vulnerabilities. Numerous network intrusions have been effectively prevented in the past. Detecting new and undisclosed attacks that are unknown is a difficult task, despite the existence of well-defined rules on these network attack types. This is due to the disparity in the transmission of data over networks, the broadcast of product patterns, the zero-afore advantage, and the breach of reactivity (Ma et al., 2016). A DoS attack, which is a type of throttling attack and concentration, is feasible in the field of network traffic categorization using ML approaches. The objective of DoS/DDoS is to saturate the network that transmits the attack with a variety of machines, thereby increasing the burden and causing congestion. Additionally, a Capture the Flag (CTF) strategy may be implemented, in which participants endeavor to assume control and establish a network or a specific data transmission path to identify the accurate proprietor of the data and ultimately achieve their objectives.

2.2 Intrusion Detection Systems (IDS)

AIDS mechanism constantly analyzes packets and detects threats from the inside and outside of the network by examining the data entering and/or departing the network. The gathering and analysis of data from multiple networks and systems sources to recognize illegal activity and access to a PC, server, or system is a method employed by IDS (Al-Turaiki and Altwaijry, 2021). The IDS may be created using machine learning-based methods, statistical approaches, and data mining to use in information technology as well as telecommunications to indicate when individuals and systems are (or are potentially) attempting to breach the policy). There are two types of IDSs-Anomaly-based IDS and Signature-based IDS. An IDS is an apparatus or program designed to prevent illegitimate approach, telecommunications, or motion throughout a network or from inside a network through many security systems. It can serve as one component of a boundary security system or as a boundary security system itself (Ahmed et al., 2022). The capacity to identify such activity is a fundamental attribute of IDS. In most cases, the IDS operate passively, alerting users or administrators only upon detecting individuals engaging in banned activities. Network security is crucial since it guarantees confidentiality, integrity, and availability. Network security is perhaps the paramount topic of concern. Networks can transmit data across public channels, making conversations susceptible to interception, alteration, or interference. Measures have been implemented to prevent intruders in recent years. These systems employ IDS technology to safeguard the network (Gao et al., 2020).

3 Deep Learning Models for Wireless Security

Conventional security solutions are constrained and fail to address emerging cyber technology trends; hence, the current circumstances necessitate extensive research into unique wireless security technologies to combat these advanced assault techniques. Recently, the DNA of intelligence in artificial intelligence has garnered significant attention to mitigate cyber security threats. Various machine learning technologies, including deep learning, reinforcement learning, semi-supervised learning, and transfer learning, are increasingly prevalent in cyber security. However, the conventional wireless security frameworks present the following issues: fault tolerance, intrusion detection, and resistance against sophisticated persistent attacks, necessitating adjustments to the implementation matrix to address cyber adversities. Currently, the extensive utilization of wireless networks promotes the implementation of numerous applications and services that epitomize the digital revolution (Ma et al., 2016). The growing prevalence of smartphones, mobile applications, IoT devices, and the expansion of remote education and employment, together with other aspects of digital transformation, necessitate and promote the

ongoing implementation of new wireless networks and services. A considerable proportion of these digital activities entail repetitive data transmission, such as internet browsing, social media data sharing, distributed file sharing, and other data-intensive applications (Javeed et al., 2021). This data-intensive cyber infrastructure depends on the strength of the wireless security framework. Nonetheless, the emergence of increasing cyber dangers and advanced cyber-attack techniques disrupts digital communications, resulting in the loss of personal, corporate, governmental, and national sovereignty (Tandiya et al., 2018a). On one hand, the nature of wireless network traffic and the scale of the data render it quite reasonable to form the data under pictures and utilize DCNN.

In addition, CNN has a few challenges, including over fitting, issues relating to gradient descent, and hyper parameter configuring. Researchers have even shown that a problem exists when using neighborhood pixels in three-dimensional planes. Despite being more potent, DCNN, like all ML systems, is sensitive to the poisoning attempt. Consequently, crucial attempts in most of the proposed SCNN-based security detection schemes are used to decrease the effect of altered input attacks. One of the deep learning methods that may be used for wireless network security is the CNN, which is developed for image processing tasks (Zhang et al., 2019). It uses several layers of convolutions with fixed-sized filters and nonlinearities for producing more abstract representations of features. The pattern has invariants because of the system's translation. The efficacy and accuracy are significantly improved due to this. Deep convolutional neural networks function similarly to a human visual system as a feature abstraction machine. It has been experimentally shown that DCNN can be extremely effective at finding and recognizing patterns from vast and image-like data. Deep learning solutions have been investigated for numerous tasks in the field of wireless mobile networking, with a particular focus on the security aspect. Conventional security strategies frequently utilize the detection of known cyber-attacks based on signature databases (Kwon et al., 2019). This is not, however, an effective method for correctly recognizing network intrusions, particularly when it comes to malicious assaults, since their patterns have not previously been seen. As a result, an approach based on machine learning techniques has commonly been used to secure wireless networks. In recent years, the use of deep learning has been increasing in wireless network defense mechanisms due to its effectiveness. Researchers have confirmed that a high level of efficacy can be obtained through the usage of deep learning. Table 4 illustrates some papers dealing with deep learning methods according to classification and detection attacks.

Table 4: The methods for deep learning-based attack classification and detection

Method	**Dataset Used**	**Evaluation Metrics**	**Main Findings**	**Ref.**
Deep learning-based network anomaly detection	Various network traffic datasets	Accuracy, Precision, Recall, F1-Score	Effective in detecting network anomalies with high accuracy	(Kwon et al., 2019)
Recurrent Neural Networks for Intrusion Detection	Network intrusion datasets	Accuracy, Detection Rate, False Alarm Rate	RNNs are effective for sequential data in intrusion detection	(Yin et al., 2017)]
Deep Learning for Network Traffic Prediction	Network traffic datasets	Mean Squared Error, Accuracy	Improved prediction of network traffic using deep learning methods	(Hussain and Hnamte, 2021)
Deep Learning for Network Intrusion Detection System	Network intrusion datasets	Accuracy, Precision, Recall	Enhanced detection capabilities using deep learning techniques	(Al-Marri et al., 2020)
GAN-based Network Intrusion Detection	Network intrusion datasets	Accuracy, Precision, Recall, F1-Score	GANs can generate realistic attack data and improve detection accuracy	(Balamurugan et al., 2022)

3.1 Implementation Details

Although the proposed models demonstrate a strong potential to improve the safety of the wireless network through deep learning techniques, implementation details require greater elaboration for reproducibility and clarity. In future versions of this work, a comprehensive explanation will be provided with respect to the architecture of the deep learning models used, including the number of layers, the types of activation functions, the regularization techniques (for example, abandonment, normalization by lots) and the structure of each model (CNN, RNN, GAN, etc.).

The training process will also be described in detail, specifying the optimization algorithm used (such as ADAM or SGD), the learning rate, the size of the lot, the number of times and any early detention criteria. In addition, the methodology for the selection of parameters will be addressed, either through manual adjustment, grid search or random search. Data preprocessing steps will be discussed, such as standardization, categorical variables, and the management of missing valuesand class equilibrium techniques such as smote or subsample. In addition, a detailed description of the data sets will be provided (including CICIDS2017, AWID3, NSL-KDD and UNSW-NB15), with clear information about the number of samples, types of covered attacks and how the data were divided into training, validation and test sets. This detailed clarification will improve the transparency and reproducibility of research, providing a stronger basis for greater development and comparison. The implementation details of the proposed learning models are summarized in Table 5, including the training process, the selection of parameters, the data preprocessing methods and the data sets used.

Table 5: Details of Implementation of the Proposed Models

Aspect	**Description**	**References**
Frameworks Used	TensorFlow 2.8, Keras	(Yin et al., 2017; Al-Marri et al., 2020)
Hardware Configuration	Intel Core i7 CPU, 32 GB RAM, NVIDIA GTX 1080Ti GPU	(Li et al., 2020)
Optimization Algorithm	Adam Optimizer with an initial learning rate of 0.001	(Li et al., 2020; Al-Marri et al., 2020)
Loss Function	Categorical Cross-Entropy	(Al-Marri et al., 2020; Hu et al., 2020)
Training Epochs	50	(Li et al., 2020; Hu et al., 2020)
Batch Size	64	(Al-Marri et al., 2020; Hu et al., 2020)
Hyperparameter Tuning	Grid Search and Random Search used for adjusting layers, neurons, learning rate, dropout rate	(Li et al., 2020; Nafti and Jemili, 2024)
Regularization Methods	Dropout (rate = 0.5), Batch Normalization	(Hu et al., 2020; Podder et al., 2021)
Preprocessing Techniques	Min-Max Normalization, One-Hot Encoding for categorical features, SMOTE for class imbalance	(Gong et al., 2024; Hu et al., 2020; Podder et al., 2021)
Datasets Used	CICIDS2017 (79 features, 15 attack types), NSL-KDD (41 features), UNSW-NB15 (49 features), AWID3 (802.11 network traffic)	(Chatzoglou et al., 2022; Gong et al., 2024; Hu et al., 2020)
Dataset Splitting	70% training, 15% validation, 15% testing	(Hu et al., 2020; Nafti and Jemili, 2024)
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score	(Kwon et al., 2019; Al-Marri et al., 2020; Hu et al., 2020)

3.2 Experimental Results and Comparison with Existing Studies

To evaluate the effectiveness of the wireless attack detection model based on proposed learning, a series of experiments were carried out using reference data sets, including CICIDS2017, NSL-KDD, UNSW-NB15 and AWID3. The proposed model performance was evaluated using standard evaluation metrics: precision, precision, withdrawal and F1 score. The results were compared to those of the latest generation intruder detection systems based on conventional automatic learning and deep learning methods. The proposed model achieved significant improvements both in the accuracy of detection and in classification reliability, particularly in the identification of minority class attacks such as U2R and R2L in the NSL-KDD data set and advanced threats such as botnet or heart attacks in CICIDS2017.

Table 6: Comparison of Proposed Model with Existing Studies

Model / Study	**Dataset**	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**Ref.**
Random Forest (Baseline)	NSL-KDD	89.21	87.56	85.14	36.34	(Yin et al., 2017)
CNN-Based IDS (Al-Turaiki et al.)	NSL-KDD	91.37	90.24	88.90	89.56	(Al-Turaiki and Altwaijry, 2021)
RNN with Attention (Yin et al.)	CICIDS2017	93.45	91.02	90.50	90.76	(Yin et al., 2017)
GAN+ Deep Autoencoder (Proposed)	CICIDS2017	96.84	95.32	94.85	95.80	This study
Hybrid CNN+SVM (Junaidi et al.)	AWID3	92.80	91.00	89.70	90.34	(Junaidi et al., 2022)
Deep Belief Network (Belarbi et al.)	UNSW-NB15	93.25	92.60	91.10	91.84	(Belarbi et al., 2022)
Deep Learning Ensemble (Proposed)	UNSW-NB15	95.40	94.35	93.70	94.02	This study

As shown in Table 6, the proposed deep learning framework outperforms traditional and

standalone machine learning models in almost all metrics across multiple datasets. The use of generative adversarial networks (GANs) and hybrid architectures contributes to better generalization and improved detection of unknown or zero-day attacks, a critical factor in real-world wireless environments. These results demonstrate that integrating deep learning with advanced feature synthesis and model optimization techniques offers a robust solution for next-generation wireless security frameworks.

4 Wireless Network Traffic Analysis

Wireless networks play a key role in modern mobile communication, ranging from mobile devices like smartphones to a variety of other wireless communication gadgets (Hu et al., 2020; Restuccia et al., 2020). Despite their popularity, wireless networks are susceptible to a myriad of security challenges. One of the most critical of these challenges is network attack detection. To ensure the integrity of wireless networks, there is a threat detection and prevention system. In the past few years, deep learning has gained popularity in several wireless-specific security contexts like physical-layer security and wireless physical-layer security. Wireless network security mainly consists of three types: MAC frame attacks, router attacks, and DoS attacks. The wireless network serial attacks are also aggregated into a variety of network attacks, and several countermeasures for the network attacks are also described in the wireless network security challenge. DL can be a better solution to enhance the classification by purely relying on the wireless intrusion deterring system (WIDS). There are some other models like Sonat et al., DUAS, WILSAC, and Aggarwal et al., but these models can be classified as class-based models. To evaluate the performance of the proposed deep learning model on the real-field datasets, the extracted standard datasets must be used on the wireless network traffic classifier and IDS (Hu et al., 2020). The CICIDS2017 dataset is an advanced malicious and normal dataset that is compiled from real-time network packets to build advanced IDS to avoid network security. The dataset consists of about 79 features and more than 80,000 data instances, and the number of instances recorded fewer than 15 kinds of attacks and 10 kinds of normal data.

The CICIDS2017 dataset is an advanced malicious and normal dataset that is compiled from real-time network packets to build advanced IDS to avoid network security. The dataset consists of about 79 features and more than 80,000 data instances, and the number of instances recorded fewer than 15 kinds of attacks and 10 kinds of normal data. The CICIDS2017 dataset matches real-world network data Packet Capture (PCAPs) and utilizes CICFlowmeter-V3.0 to extract features and labels. This dataset displays 25 users' abstract sentiments towards HTTP, HTTPS, FTP, SSH, and email protocols. Data are collected throughout time. This dataset includes attacks such as brute force FTP, SSH, DoS, heartbleed, web infiltration, botnet, and DDoS, which are not present in the other datasets. The UNSW-NB15 dataset is an advanced malicious and normal dataset, which contains all published traffic of the Intelligence Advanced Research Projects Activity (IARPA) from October 2012 to March 2013 (Gong et al., 2024). The features are 49 in numbers recorded under attacks that contain 9 classes and 4 classes of verification. The NSL-KDD dataset is designed to build a network-based IDS (NIDS) model to detect attacks. The dataset consists of about 41 features and the number of instances recorded fewer than 23 kinds of attacks. The classification of attacks mainly consists of the following three main categories: DoS, remote to user (R2L), and user to remote (U2R).

4.1 Packet Inspection Techniques

Deep packet inspection (DPI), sometimes referred to as packet sniffing, analyzes data packets traversing a network checkpoint. During conventional stateful packet inspection, the device just examines the packet header, encompassing the destination IP address, source IP address, and port number. DPI examines more metadata and data for each packet with which the device

interacts. This DPI definition involves the examination of packet headers and data. Deep packet inspection enhances the efficacy of network packet filtering. DPI may identify concealed threats in the data stream, including data exfiltration, violations of content policies, malware, and more, alongside packet-sniffing tools.

Clustering is performed on the equilibrium packets, i.e., legitimate or illegal equivalents, so new dynamically amplified data packets with the latest manuals are inspected for the dataset before inspection. The FF tradition surveyed the disadvantage of certain versions for which the favored strategies are equipped and then assessed the strengths and expense of the merchandise inspection techniques that were cited in the concluding segment. The residual neural network also adds an extra stratum of control to the software elucidation by supplying the reliability estimation after this data inspection for state espionage methods in network appraisal tactics so that it meets maximum interest by the wireless network research community, including the wireless obstructions. The multi-modal machine learning inspection methods could execute custom-made bottlenecks, and such inspection techniques submit to the features' assortment capability. Furthermore, the machine knowledge systems of traffic inspection methods remain in two classes: numerical categorization and semantic inspection (Junaidi et al., 2022). A packet inspection is an extensive study to mandate numerous advantages of packet analysis, specifically dissimilar categories of category inspection techniques. The vulnerabilities resembling host-centered, network, and behavior-based forms and the diffusion of machine learning models were examined by the review of illicit traffic and the network attacks. An overview of the catalog of accumulated datasets: the number of apparent and undisturbed network connections related to the dataset were inspected and possessed in the subsequent group to detect system strategies of traffic inspections. Few communal sensors of injected datasets, including the sensors of level seven encryptions through the costless as well as paid versions of the statistical network monitor and noise commotion processing, as well as the real-purpose sensor from these naturally trusting.

5 Advanced Classification Techniques

The physical layer status of wireless channels, resonance inside the network, and all attacks' data are other effective criteria. There is a consecutive low number of research studies that provide such practical solutions. While no action can be observed in the physical layer and no network depth can be found, the useful technique for providing effectiveness is modular. As a hardware implementation, a number of researchers have advised a multi-hop DNN (Deep Neural Network). A number of individual researchers have suggested forming a mathematical module in this system. For such systems applying low-cost sensors and hardware, a wide range of exploitation in the mathematical layer with the hardware implementation can be observed. The blocking feature in some presented models can increase the performance but will lead to an increase in latency. Consequently, these methods encourage the researcher to increase the current performance while remaining less cutting-edge than the existing systems.

Due to the negative and undesired issues like DoS, MITM, and DDoS attacks, now networks and security professionals are urging to find more possible attacks and thus improve the current classification to assure wireless security. As the different behaviors of each attack, the type of data sources, and the size of data sources affect the classification's performance, it is essential to provide a combination of deep learning and traditional machine learning techniques for enhanced classification (Javeed et al., 2021). To the best of our knowledge, the most promising approach for enhancing the classification of attacks in networks is to provide deep learning approaches in different forms and views (Al-Turaiki and Altwaijry, 2021). The big role of population-based methods, including Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Cuckoo Search (CS), Brain storm optimization (BSO), Synchronous Parallel Line Search (SPLS) and Mine blast algorithm (MBA) is another curve in the deep learning 2D charts. In the next section, these issues will be explained, and the existing solution will be offered. Here, we

provide a concise guide to the combination of deep learning and traditional machine learning techniques for enhanced classification of the most common network attacks. We have provided the most recent, promising research for both parts. We have also explained why such methods are preferred and how the existing solutions are provided. We believe that the information provided might be useful and helpful.

5.1 Support Vector Machines (SVM)

SVM can be used to detect Sybil attacks in vehicular ad hoc networks by classifying driving patterns of vehicles (Nafti and Jemili, 2024). The method developed by Aung et al. used a variety of features, including the inter-distance and relative velocity between vehicles, collected by GPS-based modules. Specifically, the extended SVM classifier was used, which is intended specifically to deal with three-class problems. The binary SVM classifier, RBF kernel, was applied to the extended class. When classifying each vehicle as either a normal vehicle, a car-following vehicle, or a malicious vehicle, the extended SVM classifier was then used. The authors reported that the number of support vectors generated by the SVM model to detect Sybil attacks was 22. SVM has also been used to validate the countermeasures proposed to secure wireless communication protocols. This is the case in the study carried out where SVM was used to validate the proposed statistical global and receiver-based thresholding for multiuser (MIMO and non-MIMO) space-time block codes (STBCs). On the other hand, an adaptive deep learning feature selection approach to detect network intrusion was proposed in the work discussed in **?**. A study that showcased the INTSet deep belief network (DBN) approach proposed to detect ship targets with wireless communication signals is discussed in Liu and Huang Zhang et al. (2019). Various machine learning models were trained, within which an SVM model was tested on the classified data obtained from the DBN model. SVM is a widely used technique in supervised machine learning for data classification Mohan et al. (2022). The work in distributed wireless network security proposed by Ma et al. (2016) presented a method using the k-nearest neighbor (k-NN) and SVM classifiers to detect the primary user emulation (PUE) attack in cognitive radio networks (CRNs).

5.2 Recurrent Neural Networks (RNNs)

Intrusion detection systems are key to network security, and there are two types of IDSs: signature-based detection (SBD) and anomaly-based detection (ABD). ABD is an effective complement to the SBD when the network encounters new and unknown attack types. At the same time, the sequential nature of network traffic data requires the capability to model the complex temporal dependency. In terms of RNNs' ability to recognize data when reliable and their effectiveness in time series tasks, RNNs are often used for ABD in networks. This unique capability helps RNNs to recognize traffic connectivity types in sequence with normal functions containing both known and unknown attacks. Various models and techniques, such as RNNs, are used in deep learning. In particular, RNNs are successfully applied to solve complex dynamic network problems, such as time series forecasting, gaming, and sequencing. When used for network intrusion detection, RNNs can thoroughly analyze the behavior and structure of network connections to detect any intrusive activity. RNNs are used in various applications such as anomaly-based intrusion detection, malware traffic classification and attack detection in Fog-to-Things computing (Kwon et al., 2019) Attacks on these networks are becoming more serious due to the move of wireless technology high and associated developments in wireless networks therefore, crisis researchers and practitioners are involved in new technologies to enhance wireless security and cope with the challenges posed by network attacks. One such approach, deep learning, has shown significant advantages in enhancing security through wireless network attack detection and advanced classification (Podder et al., 2021). Deep learning shares various similarities with Artificial Neural Networks (ANNs). However, deep learning models can learn intricate and ab-

stract data characteristics with optimal performance and little formalization (whereas ANNs struggle with complex data sets and require extensive feature engineering). As a result, deep learning has surpassed traditional machine learning methods in many domains (Gupta et al., 2022).

6 Performance Evaluation and Metrics

The Precision, Recall and F1-Score (Kwon et al., 2019): Precision quantifies what the classifier has labeled with class 1 and how many instances that does contain a 1, while recall quantifies, on the other hand, how many instances that are 1 and how many got labeled with a 1. In the case of binary classifiers, a threshold can be set at one point to minimize any of the variables, whereas in the scenario where there is a trade-off between these variables, the problem of multi-class problems is that the threshold is to be set after much discussion between them. This potential is dependent on client priorities. The F1-Score is the harmonic average of the two in the event we wish to summarize as a single performance measure. The performance of any model or classifier is a clear evaluation of its overall ability to detect the network attack effectively and accurately. There are various metrics available to evaluate the performance of a classifier. The commonly used evaluation metrics include accuracy (Xie et al., 2022). It refers to the ratio of correctly predicted observations to the total observations. It determines the percentage of times the prediction is correct. It delivers the ratio of true results, either the true positive or the true negative. The measures are not good for imbalanced data because they do not reflect those labeled instances of the minority class. In such cases, subsequently, other measures come into play since the datasets are imbalanced; accuracy is possibly insufficient to conclude for the classifying classifier (Belarbi et al., 2022). A false sense of achievement can be mainly due to usually classifying the prominent classes without really growing the correspondingly true for the other class in any of the two-class problems.

6.1 Accuracy, Precision, Recall

The recall evaluates the ability of the classifier to detect all positive samples. In other words, it quantifies the percentage of samples correctly detected as positives by the classifier. The F1-score is the weighted harmonic average of the precision and recall. A good F1-score indicates low false positives and low false negatives, like precision and recall. In these performance measures, the term 'true positive' (TP) refers to the number of positive samples that are correctly identified by the test sample. The term 'true negative' (TN) refers to the number of negative samples that are correctly identified by the test sample. The term 'false positive' (FP) refers to the number of negative test samples identified as positive by the classifier, and the term 'false negative' (FN) refers to the number of positive test samples identified as negative by the classifier. Accuracy, precision, recall, and F1-score are performance evaluation measures that are considered critical in domains like network attack detection. These performance measures are used in the interpretation of confusion matrices. The accuracy is an evaluation measure that calculates the ratio of the number of right predictions across all the samples to all the samples (Choi et al., 2020). Accuracy can be misleading at times, giving the idea that detection of different attacks provides satisfactory results (Aljabri et al., 2021). Furthermore, imbalanced datasets working on accuracy may affect classifier utilization, inflating the detection of the majority class instead of minimizing minority class detection. Therefore, the use of other performance measures (e.g., precision, recall, and F1-score) becomes critical. In this study, precision quantifies the ability of the classifier not to label a sample positive if it is negative (da Silva et al., 2022). In other words, the proportion of a sample being correctly identified as positive by the classifier is quantified by precision.

7 Challenges and Future Directions

Although different applications based on deep neural networks have shown promising features, trustworthy solutions are likely to be initiated in all sectors, given the high data rates and sensitive information present in mobile computing solutions. To enable successful secure service uptake, independent and third-party verifications of all the deep learning-based models must be done in all of the cases. Therefore, the first step is to write an outline for company/university IP rights protection and explore the possibilities of using these models in a controlled manner, with the help of regulatory authorities. With the capabilities of deep neural networks, we foresee elite algorithm enhancement in several mobile networking domains with time (Ruzomberka et al., 2023). Undoubtedly, with widespread training data from different service providers, formations can show significant generalization and can even be upgraded to include distributed learning on mobile hardware devices. This way, in a large-scale massive deployment, the mobile device can continually improve its learning robustness. However, after potential success in this domain, there should be a determined focus on the ongoing optimization of models to decrease the precision and architecture of the deep neural messages used, which is especially crucial in power-constrained mobile edge computing solutions. In addition, the centralized training scenario was assumed in all of the discussed mobile network training. Nonetheless, considering this to be a potential security concern, future work is likely to explore edge-device learning with authenticated mobile devices safely. Challenges and future directions: Deep learning models are trained and tested based on existing and clean samples (Alhoraibi et al., 2023b). These approaches might not be efficient in adversarial environments or under mild changes in channel and network configuration conditions. Tree-based models and the proposed deep learning models are trained offline based on the considered features. In dynamic environments, the performance of these models might not be consistent. Moreover, the energy and complexity of the deep neural models can further be optimized to be gesture efficient since the mobile computing solution always has resource constraints (Restuccia et al., 2020). Rule-based models might be deployed as a relatively efficient and lighter solution for anomaly detection on resource-constrained devices like mobile phones and a good combination. If available in real mobile hardware, the proposed deep learning models can be deployed as light models by considering model distillation, quantization, and pruning of the model to enhance energy efficiency and reduce the complexity of the model.

7.1 Scalability and Deployment Issues

Another important factor in the wireless deployment of advanced threat detection techniques is its scalability, particularly when dealing with dynamic network environments with an ever-increasing number of wireless nodes. The communication schemes of such models should be effective against adversarial attacks across various environmental and physical conditions. An immediate requirement, however, is obtaining guaranteed or provable effectiveness of such model communication systems against adversarial attacks and noise for wireless networks. Integrating as well as tailoring AI/ML approaches within wireless system architectures could be a step in this direction. The complexity of AI/ML models deployed for network security at the wireless edge also needs special consideration (Malhotra et al., 2021). However, DL architectures and models have evolved, now involving different compression and optimization techniques both on the model front and on the data front. Especially interesting are the deep learning models trained with knowledge distillation and post-trained by network pruning. Over time, the deployment of efficient and accurate DL models for wireless security has led to massive academic attention (Wazirali et al., 2021). However, at the same time, it has raised the concern to effectively put these complex models into practice. One major aspect of such deployment, particularly in the context of resource-constrained wireless nodes, is the model footprint; this refers to the size of the model in terms of memory and deployment cost. Towards efficient deployment, literature has

suggested that the key architecture of the model should be lightweight, that is, efficient in terms of model size and computation due to the resource-constrained environments data (Ruzomberka et al., 2023).

8 Conclusion

In conclusion, the integration of deep learning techniques into wireless security systems presents a promising avenue for enhancing network attack detection and classification. Through the utilization of advanced machine learning algorithms, such as convolutional neural networks and generative adversarial networks, researchers have made significant strides in fortifying wireless sensor networks against evolving cyber threats. The development of hybrid security analysis systems combining model-checking techniques with deep learning has shown promise in improving malware detection in IoT applications. Moreover, the application of deep learning models for cyber-attack prediction and network intrusion detection has demonstrated the potential to bolster the overall security posture of wireless networks. By leveraging the capabilities of deep learning alongside traditional machine learning approaches, researchers can achieve more accurate and efficient classification of network attacks, paving the way for enhanced security measures in the wireless communication domain. Moving forward continued research and innovation in the field of deep learning for wireless security are essential to staying ahead of emerging cyber threats and safeguarding critical wireless infrastructure.

References

Aguiar-Pérez, J. M. and Pérez-Juárez, M. Á. (2023). An insight of deep learning based demand forecasting in smart grids. *Sensors*, 23(3):1–30.

Ahmad, R., Wazirali, R., and Abu-Ain, T. (2022a). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors*, 22(13):1–35.

Ahmad, R., Wazirali, R., and Abu-Ain, T. (2022b). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors*, 22(13):1–35.

Ahmed, N., Ngadi, A. b., Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Ullah, S. S., et al. (2022). Network threat detection using machine/deep learning in sdn-based platforms: a comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction. *Sensors*, 22(20):1–34.

Al-Marri, N. A. A.-A., Ciftler, B. S., and Abdallah, M. M. (2020). Federated mimic learning for privacy preserving intrusion detection. In *2020 IEEE international black sea conference on communications and networking (BlackSeaCom)*, pages 1–6. IEEE.

Al-Turaiki, I. and Altwaijry, N. (2021). A convolutional neural network for improved anomaly-based network intrusion detection. *Big Data*, 9(3):233–252.

Alam, S. and De, D. (2014). Analysis of security threats in wireless sensor network. *arXiv preprint arXiv:1406.0298*.

Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., Khan, S., Zainal, A., and Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: a survey. *Sensors*, 22(4):1–15.

Alhoraibi, L., Alghazzawi, D., Alhebshi, R., and Rabie, O. B. J. (2023a). Physical layer authentication in wireless networks-based machine learning approaches. *Sensors*, 23(4):1–34.

Alhoraibi, L., Alghazzawi, D., Alhebshi, R., and Rabie, O. B. J. (2023b). Physical layer authentication in wireless networks-based machine learning approaches. *Sensors*, 23(4):1–34.

Aljabri, M., Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M., Aboulnour, M., Alomari, D. M., Alhamed, D. H., and Altamimi, H. S. (2021). Intelligent techniques for detecting network attacks: review and research directions. *Sensors*, 21(21):1–43.

Altaf, F., Islam, S. M., Akhtar, N., and Janjua, N. K. (2019). Going deep in medical image analysis: concepts, methods, challenges, and future directions. *IEEE access*, 7:99540–99572.

Baishya, N. M. and Manoj, B. (2024). Adversarial robustness of distilled and pruned deep learning-based wireless classifiers. In *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 01–06. IEEE.

Balamurugan, N. M., Kannadasan, R., Alsharif, M. H., and Uthansakul, P. (2022). A novel forward-propagation workflow assessment method for malicious packet detection. *Sensors*, 22(11):1–21.

Basu, D., Gu, T., and Mohapatra, P. (2020). Security issues of low power wide area networks in the context of lora networks. *arXiv preprint arXiv:2006.16554*.

Belarbi, O., Khan, A., Carnelli, P., and Spyridopoulos, T. (2022). An intrusion detection system based on deep belief networks. In *International Conference on Science of Cyber Security*, pages 377–392. Springer.

Bhatti, D. S., Saleem, S., Imran, A., Iqbal, Z., Alzahrani, A., Kim, H., and Kim, K.-I. (2022). A survey on wireless wearable body area networks: A perspective of technology and economy. *Sensors*, 22(20):1–47.

Boni, K. R. C., Xu, L., Chen, Z., and Baddoo, T. D. (2020). A security concept based on scaler distribution of a novel intrusion detection device for wireless sensor networks in a smart environment. *Sensors*, 20(17):1–20.

Castelli, M., Manzoni, L., Espindola, T., Popovič, A., and De Lorenzo, A. (2021). Generative adversarial networks for generating synthetic features for wi-fi signal quality. *Plos one*, 16(11):1–30.

Chatzoglou, E., Kambourakis, G., Smiliotopoulos, C., and Kolias, C. (2022). Best of both worlds: Detecting application layer attacks through 802.11 and non-802.11 features. *Sensors*, 22(15):1–20.

Choi, Y.-H., Liu, P., Shang, Z., Wang, H., Wang, Z., Zhang, L., Zhou, J., and Zou, Q. (2020). Using deep learning to solve computer security challenges: a survey. *Cybersecurity*, 3:1–32.

da Silva, L. M., Menezes, H. B. d. B., Luccas, M. d. S., Mailer, C., Pinto, A. S. R., Boava, A., Rodrigues, M., Ferrão, I. G., Estrella, J. C., and Branco, K. R. L. J. C. (2022). Development of an efficiency platform based on mqtt for uav controlling and dos attack detection. *Sensors*, 22(17):1–20.

Gao, M., Ma, L., Liu, H., Zhang, Z., Ning, Z., and Xu, J. (2020). Malicious network traffic detection based on deep neural networks and association analysis. *Sensors*, 20(5):1–14.

Gong, Y., Zhu, M., Huo, S., Xiang, Y., and Yu, H. (2024). Enhancing cybersecurity resilience in finance with deep learning for advanced threat detection. *arXiv e-prints*, pages arXiv–2402.

Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., and Huang, K.-Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors*, 22(5):1–34.

Hamza, A. A., Abdel Halim, I. T., Sobh, M. A., and Bahaa-Eldin, A. M. (2022). Hsas-md analyzer: a hybrid security analysis system using model-checking technique and deep learning for malware detection in iot apps. *Sensors*, 22(3):1–33.

Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., and Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEe Access*, 8:104650–104675.

Hu, H., Liu, Z., and An, J. (2020). Mining mobile intelligence for wireless systems: a deep neural network approach. *IEEE Computational Intelligence Magazine*, 15(1):24–31.

Hussain, J. and Hnamte, V. (2021). A novel deep learning based intrusion detection system: Software defined network. In *2021 International Conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, pages 506–511. IEEE.

Javeed, D., Gao, T., Khan, M. T., and Ahmad, I. (2021). A hybrid deep learning-driven sdn enabled mechanism for secure communication in internet of things (iot). *Sensors*, 21(14):1–18.

Junaidi, D. R., Ma, M., and Su, R. (2022). Secure vehicular platoon management against sybil attacks. *Sensors*, 22(22):1–29.

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., and Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing*, 22:949–961.

Li, M., Wang, Y., Wang, Z., and Zheng, H. (2020). A deep learning method based on an attention mechanism for wireless network traffic prediction. *Ad Hoc Networks*, 107:1–34.

Ma, T., Wang, F., Cheng, J., Yu, Y., and Chen, X. (2016). A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. *Sensors*, 16(10):1–23.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., and Hong, W.-C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, 21(5):1–33.

Mohan, P. V., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., and Seo, J. T. (2022). Leveraging computational intelligence techniques for defensive deception: a review, recent advances, open problems and future directions. *Sensors*, 22(6):1–26.

Nafti, I. and Jemili, I. (2024). Platooning authentication and group key generation scheme with intermittent v2i connectivity. In *2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA)*, pages 1–6. IEEE.

Podder, P., Bharati, S., Mondal, M., Paul, P. K., and Kose, U. (2021). Artificial neural network for cybersecurity: A comprehensive review. *arXiv preprint arXiv:2107.01185*.

Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R.-A., and Raboaca, M. S. (2022). Blockchain for future wireless networks: A decade survey. *Sensors*, 22(11):1–36.

Restuccia, F., D'Oro, S., Al-Shawabka, A., Rendon, B. C., Chowdhury, K., Ioannidis, S., and Melodia, T. (2020). Generalized wireless adversarial deep learning. In *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*, pages 49–54.

Ruzomberka, E., Love, D. J., Brinton, C. G., Gupta, A., Wang, C.-C., and Poor, H. V. (2023). Challenges and opportunities for beyond-5g wireless security. *IEEE Security & Privacy*, 21(5):55–66.

Shukla, P. K., Silakari, S., Bhadouria, S., and Sharma, S. (2009). A survey for designing attack resilient and adaptive medium access control protocol for wireless networks. In *2009 First International Conference on Computational Intelligence, Communication Systems and Networks*, pages 178–183. IEEE.

Tandiya, N., Jauhar, A., Marojevic, V., and Reed, J. H. (2018a). Deep predictive coding neural network for rf anomaly detection in wireless networks. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE.

Tandiya, N., Jauhar, A., Marojevic, V., and Reed, J. H. (2018b). Deep predictive coding neural network for rf anomaly detection in wireless networks. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE.

Wazirali, R., Ahmad, R., Al-Amayreh, A., Al-Madi, M., and Khalifeh, A. (2021). Secure watermarking schemes and their approaches in the iot technology: an overview. *Electronics*, 10(14):1–28.

Xie, J., Li, S., Zhang, Y., Sun, P., and Xu, H. (2022). Analysis and detection against network attacks in the overlapping phenomenon of behavior attribute. *Computers & Security*, 121:102867.

Yin, C., Zhu, Y., Fei, J., and He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access*, 5:21954–21961.

Zhang, C., Patras, P., and Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications surveys & tutorials*, 21(3):2224–2287.

Zhang, J., Qiu, Y., Peng, L., Zhou, Q., Wang, Z., and Qi, M. (2022). A comprehensive review of methods based on deep learning for diabetes-related foot ulcers. *Frontiers in Endocrinology*, 13:1–17.