Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 05 Issue: 06 | June-2025

WIRELESS SECURITY IN IoT: A NOVEL APPROACH FOR PREVENTING MAN-IN-THE MIDDLE ATTACKS

Amrita Rastogi, Sagar Choudhary[2], Anjali Saini[3]

[1,3] Student, Department of CSE, Quantum University, Roorkee, India
[2] Assistant Professor, Department of CSE, Quantum University, Roorkee, India

---

Abstract - The Internet of Things (IoT) has rapidly transformed several industries, including transportation, smart homes, healthcare, and industrial automation. However, with the increasing reliance on the inter-relatedness of IoT devices, we face significant security threats, such as Man-in-the-Middle (MitM) attacks and Distributed Denial-of-Service (DDoS) attacks. MitM attacks allow attackers to listen to and manipulate communication between the device, leading to data exposure and unauthorized access, while DDoS attacks consume network resources, reducing device life expectancy and increasing energy usage. This research proposes a security framework to mitigate MitM and DDoS attacks in IoT and wireless sensor networks (WSNs). This framework utilizes strong encryption solutions, mutual authentication protocols, and block chain-based trust management to support security while lowering computational overhead. The proposed framework prevents unauthorized access through lightweight ciphering approaches appropriate for resource-limited IoT devices, while block chain technology utilizes a decentralized, tamper-proof ledger for device authentication based on communication logs. Proposed research identifies and discusses important security and privacy challenges: link ability, unauthorized communication, and side-channel attacks.

Keywords - IoT, Deep learning, Optimization, DDoS-Attack, Energy Consumption

Introduction:

The Internet of Things (IoT) brings together numerous In order to process and exchange information, services, individuals, networked entities, and physical infrastructure. IoT systems are dynamically dispersed and rely on information distribution and edge-based computing resources. Wireless Data transfer from IoT devices to centralized models via communication across IoT devices Automotive sensors, environmental monitors, industrial robots, security devices, medical equipment, and smart home sensors are just a few of the items that these systems allow to seamlessly communicate information. An astounding 27 billion IoT devices were in use by 2017. [1]. Because IoT devices use a variety of technologies, services, and communication protocols, managing these systems is becoming more and more difficult. The IoT environment may become vulnerable as a result of this complexity. Sensitive data may be compromised by cyberattacks. including human actions, without their awareness, or even resetting devices to unsafe configurations. Through the use of botnets—malicious networks of hacked smart devices—such assaults have the ability to undermine the security of IoT networks as well as the entire ecosystem, which includes servers, apps, websites, and social networks. IoT systems' components or communication routes may also be interfered with, immobilizing the network as a whole. Standard attack detection frameworks that can analyze attack behaviors in IoT networks are therefore desperately needed. By integrating classification and feature extraction into a single model, it is documented that deep learning (DL) has enhanced the representational power of traditional machine learning (ML) techniques and solved many of their shortcomings. Additionally, DL models do away with the necessity of human feature selection, which is a laborious process in conventional classification systems. DL tools have been used by numerous researchers to address communication-related issues in IoT devices. For example, Deep Belief Networks (DBN) have been used in Automatic Modulation Categorization (AMC) systems; however, because of their limited categorization capabilities, they frequently yield subpar results. [2] Moreover, signal modulation systems with lower processing needs are found using unsorted deep neural networks (DNN), even if convolutional procedures are still difficult to extract high-dimensional features from. [3]

Problem Statement

1. Substantial self-configuration of nodes allows them to dynamically enter or exit the network, leaving both wireless sensor networks and the networks to which they connect vulnerable to intrusion from malicious actors.
2. These malicious actors tend to capitalize on vulnerabilities to launch attacks against the network, most frequently distributed denial of service (DDoS) attacks.
3. DDoS attacks are easy to detect but difficult to stop, primarily due to the dynamic behavior of nodes.
4. However, as these devices expand at a rapid pace, cybersecurity threats have also increased, where IoT networks are susceptible to DDoS and botnet attacks that intrude through hacked communications [4], resulting in interruptions to access and privacy violations.
5. Current security frameworks are ill-equipped to identify

and mitigate initial and advanced threats on IoT systems in real-time, which puts IoT systems continually at risk.

Objective

This research paper aims to develop an IoT-based approach for detecting and preventing fake access point (AP) attacks in Wi-Fi networks. By leveraging Single Board Computers (SBC) and wireless antennas with "Soft AP" features, the study focuses on enhancing network security through air scanning techniques. [25] The proposed method ensures unauthorized APs are identified and mitigated by assigning their MAC addresses to an unauthorized Virtual Local Area Network (vLAN), preventing potential threats. A key objective of this study is to offer a cost-effective and scalable security solution that seamlessly integrates into existing network infrastructures. This eliminates the need for major modifications while providing an efficient alternative to conventional security mechanisms. Furthermore, automation of intrusion detection and response is prioritized, ensuring network administrators receive timely alerts and notifications when fake APs are detected. Future advancements include exploring sophisticated detection techniques, such as SSID security setting analysis and traceroute-based identification methods. Additionally, a user-friendly software interface will be developed to support administrators in managing and mitigating fake AP threats efficiently. This research ultimately contributes to strengthening wireless network security by delivering a practical, automated, and effective defense mechanism against fake AP attacks.

Literature Review

Denial of Service (DDoS) attacks are one of the most serious threats WSNs have to deal with, as it greatly affect the performance of the network. To keep WSNs secure and effective, researchers have explored several strategies for identifying and averting such attacks. Dr. Krishan Kumar Saluji, Taranpreet Kaur, and colleagues (2016) explored security challenges in WSNs with emphasis on DDoS attacks. It found serious threats that could disrupt the networking capability, such as wormhole, black hole, and flooding attacks. Their survey of the existing techniques identified energy consumption and high false alarm rates as issues in developing better detection systems. Shital Patil and Sangita Chaudhari et al. (2016) reviewed various applications of WSNs and how they are prone to security threats, but primarily denial-of-service attacks. They presented an upgraded Co-FAIS immunity solution based on fuzzy logic to provide protection against DDoS attacks.

Investigating the susceptibility of WSNs to attacks like DDoS, sinkhole, and blackhole due to their unsecured nature was conducted by Raksha Upadhyaya, Uma Rathore Bhatta, et al. (2016). The authors introduced a scheme that utilized Dynamic Source Routing (DSR) with an energy-based detection scheme to detect compromised nodes and remove them from the network. A shutdown scheme was proposed to eliminate compromised nodes and provide alternate paths for data transmission. The proposed scheme was validated using the Qualnet 5.2 simulator, showcasing improved resilience in the WSN. Chunnu Lal (2017) recognized an attribute of WSNs that made them susceptible to DoS attacks because of limited resources. The research highlighted the significance of energy-efficient security protocols when reviewing various detection systems. The author introduced an IDS that combines an intrusion prevention system (IPS) with a routing protocol to identify compromised nodes and prevent them from forwarding packets. The simulation conducted using NS 2.35 provided favorable results against DDoS attacks when combining the IPS with the routing protocol. The rapid advancement of the Internet of Things (IoT) has raised concerns about security challenges that necessitate threat detection mechanisms. Several models and methods have been proposed to enhance security, increase detection efficiency, and assure resilience for IoT environments. This section surveyed well-studied attack detection strategies, emphasizing both their advantages and associated challenges. Li et al. [34] proposed the Mapping UML model, which demonstrated higher accuracy, fault tolerance, and detection efficiency. Marcos et al. [36] expanded on this with a Convolutional Neural Network (CNN)-based model that displayed higher accuracy, an enhanced precision rate, and a maximum recall rate.

Methodologies Framework

Wired Equivalent Privacy (WEP) is an encryption method developed primarily to secure wireless networks. Initially, WEP utilized 64-bit encryption and has since been upgraded to support 256-bit encryption standards. [6] Of these algorithms, the 128-bit encryption algorithm was the most widelyd [6].

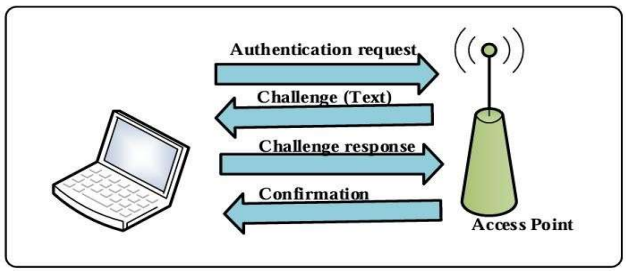


Fig.1.WEP Authentication

Then answers with a randomly generated challenge text (64 bit or 128 bit challenge, depending on the level of encryption). In 2003, the new standard brought

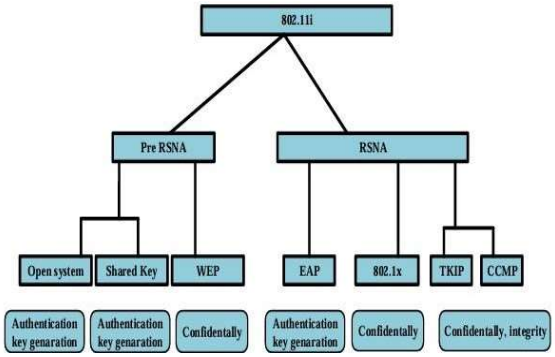


Fig.2.Classes of the 802.11i standard

The development of improved encryption mechanisms Wi-Fi Protected Access (WPA) and WPA2, which offer more advanced authentication and data protection, while still remaining backward compatible. WPA and WPA2 use stronger encryption algorithms, the Temporal Key Integrity Protocol (CCMP), respectively. These procedures were developed based on the Advanced Encryption Standard (AES) [6]. Figure 1 presents the security classes outlined under IEEE 802.11i [7].

Option 1:

Capturing the 4-way handshake:

In the case of an attacking adversary, they typically will not engage a busy network until a user engages in authentication, at which point the attacker will attempt to seize the 4-way handshake. The4-way handshake is defined in the IEEE 802.11i standard, [8] which provides secure authentication to wireless networks for both PSK (pre-shared key) and 802.1X authentication methods.

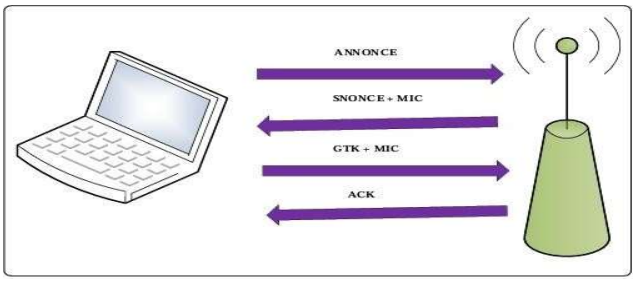


Fig. 3. WPA/WPA2 4 way handshake

The 4-way handshake occurs through four messages being sent between an AP (access point) and a client (supplicant).

Message 1 - The AP generates a random number called an ANonce (Authenticator Nonce) and sends that random number to the client.

Message 2: After receiving the ANonce, the client creates a random number known as SNonce (Supplicant Nonce). The Pairwise Transient Key (PTK) is created by the client from both nonces and the pre-shared key. The client sends the SNonce along with a Message Integrity Code (MIC) to the AP.

Message 3: The AP can now generate the PTK since it knows the values used to generate it. The AP also generates a Group Temporal Key (GTK) in addition to the PTK; this GTK is used to encrypt broadcast and multicast traffic.

Message 4: The last message that the client sends back to the AP is an acknowledgment that the client received the GTK and that the PTK was installed successfully. The end of the authentication phase is complete.

Option 2:

Deauthentication Attack Framework

A deauthentication attack represents a Layer 2 Denial-of-Service (DoS) on the IEEE 802.11 wireless technology. [9] In this attack, the attacker sends fabricated deauthentication messages to prompt an ESSAN access client to unplug from a wireless access point (AP).

Table 1. REVIEW ON TRADITIONAL ATTACK MODEL IN IOT: FEATURES AND CHALLAN

Author [citation]	Adopted scheme	Features	Challenges
Li *et al.* [34]	Mapping UML model	✓ Higher detection efficiency ✓ Fault tolerance ✓ Better accuracy	➢ The data selection sensor technique was not incorporated into the computer environment.
Boubeta, et al. [35]	CEP and ML models	✓ Better precision ✓ Higher recall ✓ Maximum F1 score	➢ More event patterns were not defined in the proposed model for detecting other types of attacks.
Marcos *et al.* [36]	CNN model	✓ Higher accuracy ✓ Improved precision rate ✓ Maximum recall	➢ Need to maximize the host count in the simulated SDN environment.
Mabodi *et al.* [37]	MTISS-IoT model	✓ Better FPR ✓ Low FNR ✓ Maximum detection rate	➢ The firefly optimization was not used in the proposed work to lower consumption energy and malicious attacks on the IoT.
Sai *et al.* [38]	MMFN method	✓ Robustness, ✓ Higher classification accuracy ✓ Strong characterization ability.	➢ The small-scale data-driven DL- AMC model with less training time was needed for training the NN.
Mohammed *et al.* [39]	IoT-based HAN model	✓ Better accuracy ✓ Reduced false positives ✓ High precision	➢ The proposed work needs to suggest the moving data process close to the network edge
Sahay *et al.* [40]	XGBoost Classifier	✓ Secured network ✓ Maximum accuracy ✓ Higher recall ✓ Improved operational efficiency	➢ Need to investigate an efficient mechanism to address and analyze the challenges.
Alabady *et al.* [41]	VLAN	✓ Effective security execution ✓ Best network speed and services	➢ The VLAN technology were not utilized in the LAN environment.

MODEL OF INTRUSION DETECTION ON IOT

IoT (Internet of Things) is a vital aspect of the current information age and a new base of information technologies. Located at the center of the IoT ecosystem is an IoT server, which is considered the functional core of the whole ecosystem. It is responsible for key functionality, such as processing terminal sensor data, aggregating data, and processing and returning that data. Security is a crucial component of today's networked digital landscape and is increasingly important as IoT technologies continue to develop.

Intrusion Detection Systems, or IDS, are essential IoT server protections. In Figure 1, you can see how significant IDS are to the IoT network protection. As IoT applications operate remotely, many IoT devices and servers are available over the public Internet, creating potential targets to cyber attackers. Attackers may exploit vulnerabilities to compromise these systems.

To respond to these threats, intrusion detection systems (IDS) are essential in identifying and defending against malicious attacks. They protect end users and service providers from several dangerous variables associated with the Internet. Nevertheless, security measures in IoT applications remain immature, and there has not been a significant reduction in the attack surface. Thus, attackers can still compromise nodes on the network.

Data collection

To identify and mitigate rogue access point attacks, it is critical to first collect relevant data from network traffic. This includes monitoring the wireless network environment—not only identifying signals of suspicious behavior. During the data collection process, data such as MAC addresses, SSID broadcasts, signal strength, types of encryption, and frequency channels are all collected. While routinely monitoring, you can identify both legitimate and malicious access points for further,

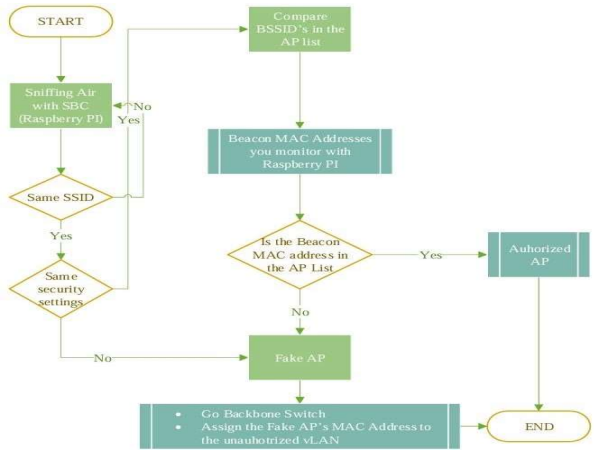


Fig. 4. Algorithm of the proposed method

Using Lightweight Access Point Protocol (LWAPP) tunnels, which also allows for centralization, the Raspberry Pi device was deployed in the target area to observe Wi-Fi transmissions. The Raspberry Pi was installed in monitor mode to passively record all nearby wireless traffic. A Raspberry Pi 3 model was used with a 16 GB Class 10 Micro SD card preloaded with the Kali Linux operating system. An ODROID module was added to the Raspberry Pi 3 to allow wireless monitoring. [23],

[24] With this module, the AirScan utility was used to scan and record surrounding Wi-Fi networks and their signals. The device had the requisite software tools set up and ready to use. After everything was deployed, the Raspberry Pi employed the method illustrated in Figure 8 to recognize any rogue behavior. In this case, rogue behavior refers to attackers who broadcast fake access points within the area being monitored.

Step 1: To aid passive monitoring of the network, the ODROID module of the Raspberry Pi 3 was initiated into monitor mode by the following command below: WLAN0 airmon-ng start The done follows: Iwconfig Figure 9 displays the output of this command, showing confirmation of the monitor mode.

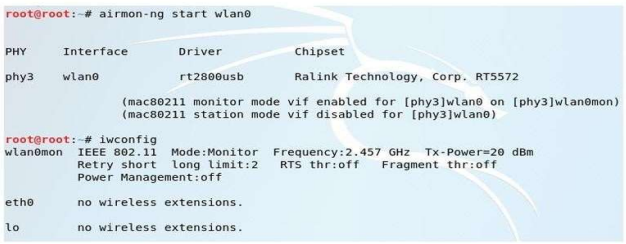


Fig. 5. Odroid module in monitor mode

Step 2: In the second phase of the assessment, the command airodump-ng wlan0mon was executed, which activates the Airscan utility. The first test scenario consisted of emulating an access point with the BSSID 00:11:22:33:44:00 and SSID FU_TEST. This SSID was selected to represent a real and legitimate network that has the same name. The important distinction is that the imitated SSID was left open with no security settings, whereas the real FU_TEST network was secured with WPA2 encryption. To fake an access point for the attack simulation, the attacker edited the hostapd-mana.conf configuration file to advertise FU_TEST as the SSID and the BSSID as 00:11:22:33:44:00.

The Raspberry Pi 3 identifies the unauthorized broadcast of a fake SSID based on the algorithm provided. The Raspberry Pi connects to the network backbone using SSH once the unauthorized VLAN is in the network infrastructure. Consequently, any users connecting to this fake SSID will not be able to access the internet and will be prohibited from communicating with people outside their local network.

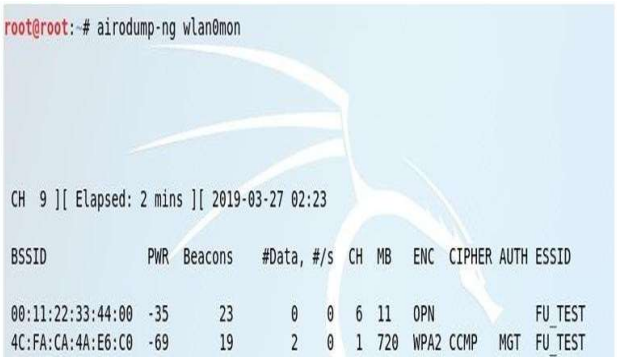


Fig. 6. Result of the first test case

Step 3: A more complex fake SSID was broadcast in the third step, with the same BSSID. This configuration was implemented in order to more closely mimic the original network and make it more challenging for users to be aware of the fake access point. As we can see in Figure 11, the Airscan began by typing the command airodump-ng wlan0mon, which acted as a watcher in the environment. Because the fake network appears authentic and protected; this type of attack is designed to covertly sniff user traffic without drawing attention to itself. In this attack scenario, an attacker decodes a fictitious access point by copying the actual FU_TEST network security protocols using the file called *hostapd-mana.conf* found in the mana-toolkit

interface=wlan0, ssid=FU_TEST; channel=6; wpa=2;

wpa_key_mgmt=WPA-EAP; wpa_pairwise=TKIP CCMP; wpa_passphrase=secure Password

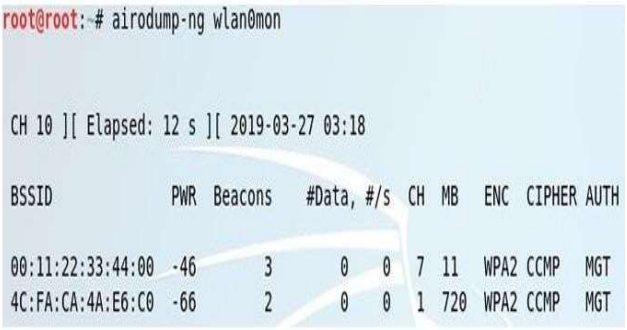
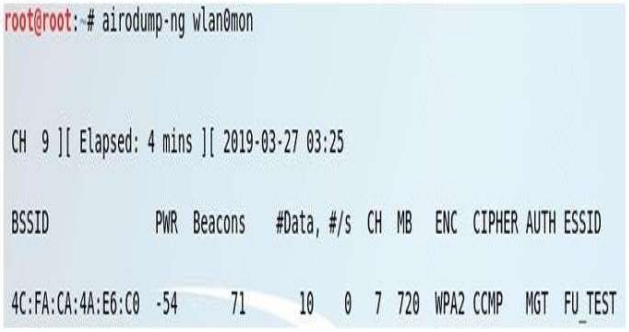


Fig. 7 Fake AP broadcast with identical security Standards as the original ssid

Step 4: To create a nearly unnoticeable fake access point, the attacker cloned the complete configuration of the real access point, including SSID, security settings, and BSSID (MAC address). This makes it very challenging for users and devices to distinguish between the legitimate access network. The output of this scenario can be seen in Figure 12.

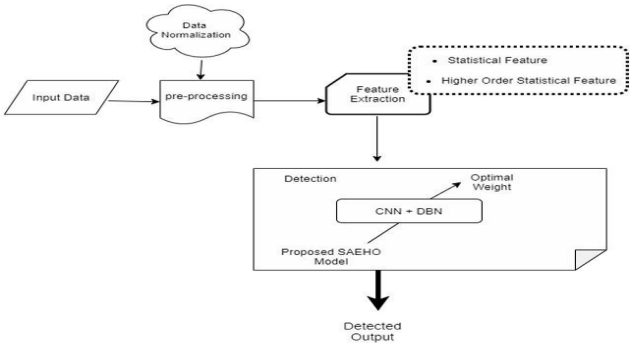
Fig. 8. Fake AP attack with same bssid, SSID and security settings



The Adopted Attack Detection Model in IoT

To guarantee consistency and enhance model performance, the input data is first normalized. Both statistics and higher-order statistical characteristics are extracted from the data during the feature Statistics include metrics such as mean, median, standard deviation (SD), mode, harmonic mean Kurtosis, skewness, energy, entropy, mean frequency, and percentile values are examples of higher-order statistical properties.

Fig. 2. Overall Framework of the Proposed Model.



Data Process:

Attack detection by Proposed Hybrid Deep Learning Model

The proposed hybrid model runs both models in parallel with the extracted set of features. The final detection result is calculated by averaging the outputs of each model.

Optimized CNN Model

The extracted features (FE) will serve as input for a modified Convolutional Neural Network (CNN) Advantages of CNN include its power, trainability, and multiple layers (stages). CNNs treat data as multiple layer structures, where each layer has a level of flexibility and builds on inferred information

from input data in the previous layer, generating feature maps [feature maps are structured arrays organized in three dimensions representing learned patterns]. [44]

The CNN I used in this model has three kinds of layers: Convolutional Layer

Pooling Layer

Fully Connected Layer Convolutional Layer

This layer has a few convolutional kernels (filters) that scan the feature maps of the input to provide characteristics in space. Each kernel produces another feature map, which is defined as created with learnable hts.ts.weights. , g, g , $x\ s = W\ s\ l\ T\ L\ e$, $g\ s + B\ s\ l$ 1)(1) H(e,g,x) = W(s,l),T = L e,g s + B s.The input patch at (e,g), denoted as WX, W, and l, will have weight W and bias term mappings and not only linear erns.patterns. $A\ e$, g , $x\ s = A$ ($H\ e$, g , $x\ s$) (2)A(e, g, x, s) = A(H)(2)

Pooling Layer

The pooling layer reduces the spatial dimensionality of feature maps, which helps the model run very efficiently while also reducing overfitting by arbitrarily discarding some activations. Common methods of pooling include max pooling (selecting the essentially the highest value only, to retain that, applied over a local neighborhood,..,.

$P\ e$, g , $x\ s$ = pool ($A\ e$, g , $x\ s$) , ∀ (c ^ , r ^) ∈ $I\ e$, g (3) P e,g,x s=pool(A e,g,x s), ∀ (c ^ , r ^)∈I e,g

Fully Connected Layer

The feature maps will later "flatten" after the pooling operation and forwarded to fully connected layers. layers. The process whereby a neuron is connected to all of the activations from the previous layer, is accomplished here. This layer, following the last convolution transfers similar data to the output layer, generates the final classification result, denoted as CL CNN.

Weight Optimization

Later, the weights from the convolutional and fully connected layers will be optimized using the Self-Adaptive Enhanced Harris Hawk Optimization (SAEHO) algorithm, which adjusts the parameters for better learning and generalization. [45]

Loss = 1 Number.

∑t=1Num P (ς ; U (t) , OUT (t)) (4) Loss = number one.

t = 1 ∑NumP(ς;U(t),OUT(t))(4)In this case, U (t) U(t) is the input at time t t, OUT (t) OUT(t)

Analysis

The paper "Wireless Security in IoT: A New Approach to Man-in-the-Middle Attacks" gives an informative and deep analysis of security vulnerabilities in the Internet of Things (IoT) and Wireless Sensor Networks (WSNs), with an emphasis on addressing MitM and DDoS attacks.A multi-layered security framework consisting of lightweight cryptography, blockchain-based authentication and intrusion detection methodology and approaches based on deep learning techniques were presented by the authors. The article provides theoretical and practical aspects using Raspberry Pi modules and ODROID modules for the purposes of rogue access point detection via air monitoring. These real-time detection methods can segregate an unauthorized or suspected MAC address into a non-permission VLAN and instigate action preventing a breach.[25] The authors present a hybrid deep learning model employing Convolutional Neural Networks (CNN) and Deep Belief Networks

(DBN), by way of a Self-Adaptive Enhanced Harris Hawk Optimization (SAEHO) algorithm to

_optimize the CNN-DBN model.[44], [45] This approach demonstrates a significant improvement to smart city NVA due to the anomaly detection in the model. The article is developed on a significant literature review and presents widening scope in a layered approach that incorporates encryption protocols (WPA/WPA2), handshake authentication analysis and signal based rogue AP detection.

Result Analysis

1. DDoS Detection in Wireless Sensor Networks. This research looks at how to identify malicious nodes that perform Distributed Denial of Service (DDoS) attacks in a wireless network with constrained resources. Such attacks can use sensor nodes' limited energy resources, likely causing catastrophic system failures - especially in mission-critical contexts such as military applications or remote monitoring environments.

Key benefits:

Identifies and finds malicious nodes for better energy efficiency and network lifetime. Engages with a timely and important research area with real-world impacts.

Strengths:

Directly relates to practice in high vulnerability settings that demand resilience in the system. Sustains the operational capability of a system by protecting limited node resources.

Limitations:

- The method is unclear, creating concerns both scalability and clarity of implementation.
- The dynamicity of WSNs with mobile nodes could hinder accurate detection of threats.

The second paper addressed a hybrid deep learning model that provides a model for detection of cyber risks in smart city IoT networks using Deep Belief Networks (DBNs) and Convolutional Neural Networks (CNNs) with the Self-Adaptive Enhanced Harris Hawk Optimization (SAEHO) algorithm to fine-tune the parameters to increase detection accuracy.

Key Contributions:

- Provides real-time threat detection capability, which is vital to the safe operation of Smart Cities.
- Provides location and time based processing of data patterns, which better supports anomaly detection.

Strengths:

- The hybrid model enhances feature extraction and achieves higher classification accuracy. Limitations:
- Scalability is a concern given the number of IoT devices in urban areas.
- Reliance on labeled datasets puts up limitations in the effectiveness against zero-day or novel attacks.
- The heterogeneity of IoT device and protocols may adversely influence model generalizability in many different situations.

Conclusion:

As a result of their greater importance for modern digital infrastructure, wireless networks are potentially at an even greater risk of developing new types of cyber threats. The study discusses the need for better wireless network security against known security threats such as DDoS (Distributed Denial of Service) attacks, as well as rogue AP (Access Point) threats. Advanced deep learning algorithms may assist in the detection and possible prevention of cyberattacks to help enhance the security of required incidence response into an even greater defense system for networks.

In summary, the first part of this research has provided a practical and efficient method for detecting and preventing fake Access Point (AP) attacks in Wi-Fi networks that are vulnerable as a result of poor configurations. By proposing an algorithm and pseudo-code, the method uses Raspberry Pi 3 and Odroid module style SBCs to effectively detect fake APs. The process will be enhanced further by creating a software application - one that is user-friendly - that can identify counterfeit APs, particularly those which replicate real security configurations and MAC addresses. This method can improve wireless security significantly by providing detection and reaction times in real-time.

Wireless Sensor Networks (WSNs) are especially susceptible to various malicious actions due to their fluid and decentralized characteristics; Distributed Denial-of-Service (DDoS) attacks are a significant concern. These attacks can dramatically affect network performance. According to this study there is an urgent need for new methods to detect, mitigate, and diminish these threats, and future work will focus on augmenting the WSN's resilience to DDoS attacks to facilitate more secure and reliable network operations.

This study describes a new hybrid deep learning model to boost the accuracy of cyberattack detection leveraging the benefits of Convolutional Neural Networks (CNN) and Deep Belief Networks (DBN), as well as an innovative algorithm, termed the SAEHO algorithm, which merges fundamental principles of the Social Optimization Algorithm (SOA) and Elephant Herding Optimization (EHO)Results from experiments demonstrate that this method significantly improves detection rates and accuracy for many cyber threats. Future work will focus on an exhaustive comparison with current models, and testing the robustness and effectiveness of the proposed system using a number of metrics.

Future scope:

Based on the outcomes of the three studies addressed, several primary trajectories for further future studies seem to enhance security in resource-constrained networks; specifically, Wireless Sensor Networks (WSNs) and IoT-enabled smart cities. These trajectories seek to augment detection capabilities, scalability, energy efficiency, and real-world applications of the security framework.

1. Enhanced and Hybrid Detection Model

Future work could examine ensemble strategies, which leverage a large number of classifiers to enhance accuracy, resilience, and generalization under various circumstances. These approaches can also assist in improving resilience against adversarial attacks by pooling the advantages of many algorithms while minimizing the chance of overfitting. [50], [51]

2. Scalability of Detection Models

The importance of scalable detection models increases when we consider the scale and complexity of IoT networks. Future research in intrusion detection should consider leveraging edge and fog computing concepts to decentralize intrusion detection. The advantage of this option is that it will eliminate the elimination. latency, reducing bottleneck for central servers, and enabling real-time threat detection for large, scalable IoT systems by off-loading processing to edge devices closer to the data sources.

3. Real-Time and Dynamic Threat Detection

Adaptive Models: IoT networks are highly dynamic, and devices are consistently connecting and disconnecting to the system. In order to be successful in tackling this dynamic nature of IoT, threat detection models have to be able to adapt to

changing topology or network structure. Continuous research could focus on building models that are a constant learning model, which can learn in real time, instead of having to be completely restrained from the beginning based on past data and recently evolving attacks.

Context-Aware Detection Systems: Another feasible and workable option is to develop context-aware detection methods. Context-aware detection systems are able to detect with respect to context

4. Enhanced data quality and reliability

Synthetic Datasets and Data Augmentation: One of the most frustrating components of machine learning-enabled attack detection for IoT systems is the scarcity of labeled data for new/unknown attack types.[44], [48] Future work could involve creating alternative synthetic datasets (i.e a standby of conceptual models) and exploring data augmentation techniques to fabricate a range of possible IoT attack instances over small spaces.

References

[1] C. Xu, W. Jin, X. Wang, G. Zhao, and S. Yu, "MC-VAP: A multi connection virtual access point for high performance software-defined wireless networks," J. Netw. Comput. Appl., vol. 122, pp. 88–98, 2018.

[2] D. Liu, B. Barber, and L. DiGrande, Cisco CCNA/CCENT exam 640-802, 640-822, 640-816 preparation kit. 2009.

[3] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, "Vulnerabilities of Wireless Security protocols (WEP and WPA2)," Int. J. Adv. Res. Comput. Eng. Technol., vol. 1, no. 2, pp. 2278–1323, 2012.

[4] H. R. Hassan and Y. Challal, "Enhanced WEP: an efficient solution to WEP threats," 2005, pp. 594–599.

[5] R. Heartfield et al., "A taxonomy of cyber-physical threats and impact in the smart home," Computers and Security. 2018.

[6] S. Wong, "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards," … ans. org/rr/whitepapers/wireless/1109. php Retrieved, pp. 1–10, 2003.

[7] S. Vibhuti, "IEEE 802.11 WEP Wired Equivalent Privacy Concepts and Vulnerability," San Jose State Univ., no. Iv, 2008.

[8] A. H. Lashkari, R. S. Hosseini, and F. Towhidi, "Wired equivalent privacy (WEP)," in Proceedings - 2009 International Conference on Future Computer and Communication, ICFCC 2009, 2009, pp. 492–495.

[9] Y. Liu, Z. Jin, and Y. Wang, "Survey on security scheme and attacking methods of WPA/WPA2," 2010 6th Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2010, pp. 1–4, 2010.

[10] A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," in Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015, 2016, pp. 165–169.

[11] J. Z. Liu Yong-lei, "Distributed method for cracking WPA/WPA2-PSK on multi-coreCPU and GPU architecture," no. November 2013, pp. 723–742, 2009.

[12] S. Gold, "Cracking wireless networks," Netw. Secur., vol. 2011, no. 11, pp. 14–18, 2011.

[13] Y. Wang, Z. Jin, and X. Zhao, "Practical defense against WEP and WPA-PSK attack for WLAN," in 2010 6th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2010, 2010.

[14] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," Computer Standards and Interfaces, vol. 31, no. 5. pp. 931–941, 2009.

[15] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions.," in USENIX security, 2003, pp. 15 28.

[16] X. Zha and M. Ma, "Security improvements of IEEE 802.11i 4-way handshake scheme," in 12th IEEE International Conference on Communication Systems 2010, ICCS 2010, 2010, pp. 667–671.

[17] Z. Bai and Y. Bai, "4-Way handshake solutions to avoid denial of service attack in ultra wideband networks," in 3rd International Symposium on Intelligent Information Technology Application, IITA 2009, 2009, vol. 3, pp. 232–235.

[18] S. H. Eum, Y. H. Kim, and H. K. Choi, "A Secure 4-Way Handshake in 802.11i Using Cookies.pdf," vol. 2, no. 1, 2008.

[19] A. Alabdulatif, X. Ma, and L. Nolle, "Analysing and

attacking the 4 way handshake of IEEE 802.11i standard," in 2013 8th International Copyright © BAJECE http://dergipark.gov.tr/bajece ISSN: 2147-284X BALKAN JOURNAL OF ELECTRICAL & COMPUTER ENGINEERING, Vol. 8, No. 1, January 2020 Copyright © BAJECE ISSN: 2147-284X http://dergipark.gov.tr/bajece Conference for Internet Technology and Secured Transactions, ICITST 2013, 2013, pp. 382–387.

[20] Internet, "4 Way Handshake." .

[21] T. D. Nguyen, D. H. M. Nguyen, B. N. Tran, H. Vu, and N. Mittal, "A lightweight solution for defending against deauthentication/ disassociation attacks on 802.11 networks," Proc. - Int. Conf. Comput Commun. Networks, ICCCN, pp. 185–190, 2008.

[22] K. El-Khatib, "Impact of feature reduction on the efficiency of wireless intrusion detection systems," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 8, pp. 1143–1149, 2010.

[23] K. F. Kao, W. C. Chen, J. C. Chang, and H. Te Chu, "An accurate fake access point detection method based on deviation of beacon time interval," in Proceedings - 8th International Conference on Software Security and Reliability - Companion, SERE-C 2014, 2014, pp. 1–2.

[24] M. K. Chirumamilla and B. Ramamurthy, "Agent based intrusion detection and response system for wireless LANs," 2004, pp. 492–496.

[25] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client-side," in Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 2012, pp. 684–687.

[26] Manhee Lee, Eun Jung Kim,Cheol Won Lee, "A Source Identification Scheme against DDoS Attacks in Cluster Interconnects", 2004, Proceedings of the 2004 International Conference on Parallel Processing Workshops (ICPP W'04)

[27] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology, vol. 2, pp. 1043-1048, 2006.

[28] S. Kumar, R. Valdez, O. Gomez and S. Bose, "Survivability Evaluation of Wireless Sensor Network under DDoS Attack", 2006, International Conference on Mobile Communications and Learning Technologies (ICNICONS CL'06)

[29] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in wireless sensor networks", WCE, vol.1, pp 5-15, 2008.

[30] Healy M, Newe T, Lewis E, "Security for wireless sensor networks: A review in Sensors Applications Symposium (SAS)", 2009 IEEE, vol. 3, pp. 80-85, 2009.

[31] Mahdi Zamani, MahnushMovahedi, Mohammad Ebadzadeh, Hossein Pedram, "A DDoS-Aware IDS Model Based on Danger Theory and Mobile Agents", 2009 International Conference on Computational Intelligence and Security.

[32] Kaur, K., &Kumari, N. Evaluation and Analysis of Active RFID Protocol in Wireless Sensor Networks, vol. 3, pp. 121-129, 2010.

[33] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, pp. 14-27, 2010.

[34] Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma, "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE 2016), vol. 4, pp. 131-140, 2016.

[35] ShitalPatila, SangitaChaudhari, "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing andVirtualization 2016, vol. 79, pp. 715-721, 2016.

[36] Raksha Upadhyaya, Uma Rathore Bhatta, HarendraTripathia, "DDOS Attack Aware DSR Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74, 2016.

[37] KatarzynaMazur, Bogdan Ksiezopolski, and Radoslaw Nielek, "Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks", 2016, Hindawi Publishing Corporation Journal of Sensors.

[38] Chunnu Lal, "a survey on denial-of-service attacks detection and prevention mechanisms in wireless

sensor networks", 2017, international journal of current engineering and scientific research (ijcesr), volume-4, issue-10.

[39] Surendra Nagar, Shyam Singh Rajput , Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).

[40] ShivamDhuria and Monika Sachdeva, "Detection and Prevention of DDoS Attacks in Wireless Sensor Networks" Springer Nature Singapore Pte Ltd. 2018.

[41]1N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE Communications Surveys and Tutorials, vol. 21, no. 3, pp. 2671–2701, Jul.2019,doi:

10.1109/COMST.2019.2896380.

[42] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," Applied Soft Computing Journal, vol. 72, pp. 79–89, Nov. 2018, doi: 10.1016/j.asoc.2018.05.049.

[43] M. Hossain and J. Xie, "Third Eye: Context-Aware Detection for Hidden Terminal Emulation Attacks in Cognitive Radio-Enabled IoT Networks," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 214–228, Mar. 2020, doi: 10.1109/TCCN.2020.2968324.

[44] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[45] A. Kore and S. Patil, "IC-MADS: IoT Enabled Cross Layer Man-in Middle Attack Detection System for Smart Healthcare Application," Wireless Personal Communications, vol. 113, no. 2, pp. 727–746, Jul. 2020, doi: 10.1007/s11277-020-07250-0.

[46] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," IEEE Access, vol. 6, pp. 24694–24705, Apr. 2018, doi:

10.1109/ACCESS.2018.2831284.

[47] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," IEEE Access, vol. 8, pp. 11743–11753, 2020, doi: 10.1109/ACCESS.2019.2959047.

[48] K. Mandal, M. Rajkumar, P. Ezhumalai,

D. Jayakumar, and R. Yuvarani, "Improved security using machine learning for IoT intrusion detection system," Materials Today: Proceedings, Dec. 2020, doi: 10.1016/j.matpr.2020.10.187.

[49] D. C. Wang, I. R. Chen, and H. Al-Hamadi, "Reliability of Autonomous Internet of Things Systems with Intrusion Detection Attack-Defense Game Design," IEEE Transactions on Reliability, vol. 70, no. 1, pp. 188–199, Mar. 2021, doi:

10.1109/TR.2020.2983610.

[50] S. Rani and N. Singh Gill, "HYBRID MODEL FOR TWITTER DATA SENTIMENT ANALYSIS BASED ON ENSEMBLE OF DICTIONARY BASED CLASSIFIER AND STACKED MACHINE LEARNING CLASSIFIERS-SVM, KNN

AND C5.0," Journal of Theoretical and Applied Information Technology, vol. 29, p. 4, 2020, Accessed: Jan. 19, 2022. [Online].

Available: www.jatit.org

[51] N. S. G. Sangeeta Rani, "Hybrid Model using Stack-Based Ensemble Classifier and Dictionary Classifier to Improve Classification Accuracy of Twitter Sentiment Analysis," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 7, 2020.

[52] P. Gulia and N. Singh Gill, "Comprehensive Analysis of Flow Incorporated Neural Network based Lightweight Video Compression Architecture," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, 2021, Accessed:

Jan. 19, 2022. [Online]. Available: www.ijacsa.thesai.org

[53] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552–9562, Oct. 2020, doi:10.1109/JIOT.2020.2993782.

[54] T. Zhi, Y. Liu, and J. Wu, "A Reputation Value-Based Early Detection Mechanism against the Consumer-Provider Collusive Attack in Information-Centric IoT," IEEE Access, vol. 8, pp. 38262–38275, 2020, doi: 10.1109/ACCESS.2020.2976141.

[55] H. Al-Hamadi, I. R. Chen, D. C. Wang, and M.

Almashan, "Attack and defense strategies for intrusion detection in autonomous distributed IoT systems," IEEE Access, vol. 8, pp. 168994–169009, 2020, doi: 10.1109/ACCESS.2020.3023616.

[56] S. Patranabis et al., "Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications," Journal of Hardware and Systems Security, vol. 3, no. 2, pp. 103–131, Jun. 2019, doi: 10.1007/s41635-018-0049-y.

[57] A. Sagu, N. Singh, G., and P. Gulia, "Artificial Neural Network for the Internet of Things Security," International Journal of Engineering Trends and Technology, vol. 68, pp. 137–144, 2020, doi: 10.14445/22315381/IJETT-V68I11P218.

[58] N. S. G. Sagu Amit, "Machine Learning Decision Tree Classifier and Logistics Regression Model," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 1.4, pp. 163–166, Sep. 2020, doi: 10.30534/ijatcse/2020/2491.42020.

[59] N. S. G. Sangeeta, "Framework for Tweet Sentiment Classification Using Boosting Based Ensemble Approach," CIENCIA E TECNICA VITIVINICOLAA SCIENCE AND TECHNOLOGY JOURNAL (ISSN: 2416-3953), pp. 1–13, 2017.

[60] S. Rani, N. S. Gill, and P. Gulia, "Analyzing impact of number of features on efficiency of hybrid model of lexicon and stack based ensemble classifier for twitter sentiment analysis using WEKA tool," Indonesian Journal of Electrical Engineering and Computer Science, vol. 22, no. 2, pp. 1041–1051, May 2021, doi: 10.11591/IJEECS.V22.I2.PP1041-1051.

[61] P. Gulia, "Performance Analysis of Advancements in Video Compression with Deep Learning," International Journal of Electrical Engineering and Technology, vol. 11, no. 5, pp. 137–143, 2020, doi: 10.34218/IJEET.11.5.2020.016.