JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Automated Wireless Attack Detection andMitigation System

[1]Saran Sanakya A [2]Dr. Prabhu A , Student, Jain (Deemed-to-be) University, Bangalore
Associate Professor, Jain (Deemed-to-be) University, Bangalore

***Abstract*—** These days, WLANs, or wireless local area networks, are quite common due to their benefits, which include portability, flexibility in location, ease of maintenance, and easier installation. On the other hand, as wireless networking penetration has increased, malevolent actors looking to take advantage of weaknesses have also become more visible. By making networks unworkable, Attacks at the wireless connection layer, which go after the lowest levels of the OSI protocol stack, are quite dangerous. Specifically, the exposing of management frames makes wireless networks more vulnerable to these kinds of assaults. Inspired by these worries, this work aims to present a novel method for identifying and mitigating wireless connection layer threats. The main goal is to put in place a strong network security mechanism designed especially to stop these assaults while learning more about their unique characteristics. In order to do this, the research proposal proposes the Wireless Link Layer Attacks Detection Algorithm (WLLADA), which combines passive and active fingerprinting techniques. The focus is on efficiently detecting denial-of-service (DoS) assaults that masquerade. The suggested approach is put into practice utilizing Python network programming and the Kali Linux environment in a real-time configuration. By using this strategy, the research hopes to reduce worries about plagiarism and provide a complex and distinctive advancement in the realm of wireless security.

Keywords—wireless, layer, WLAN Security, MAC Address, Link layer, wireless security, deauthentication.

I. INTRODUCTION

The need for communication security is paramount in the ever-changing world of wireless networks, particularly in light of WLANs' vulnerability to possible surveillance and infiltration because of their unsecured architecture. An adversarial environment is created when security measures are lax and weaknesses in data frames, management, and control are exposed. Although well-established cryptographic defences, including those provided by VPNs and 802.11i, successfully fend off crypto assaults that aim to gain unauthorized access, man-in-the-middle attacks, and eavesdropping attacks, handling Denial of Service(DoS) attacks is an ongoing issue.

Cryptography vulnerabilities and link layer attacks include the two main subsets of DoS attacks on WLANs. Through techniques like illegal access and session hijacking, crypto assaults deliberately seek confidentiality, integrity, and availability. These attacks are mitigated by established security standards. Link layer assaults, on the other hand, are more complicated to handle since they try to interfere with the wireless medium itself.

WLANs that lack encryption in their control and administration framing are vulnerable to denial-of-service (DoS) assaults, of which disassociation flooding and deauthentication are two especially disruptive techniques. The current research projects aim to decipher the complexity related to these link layer flaws. The study aims to make a substantial contribution to the body of comprehensive techniques that strengthen the resilience of Wi-Fi networks towards denial-of-service (DoS) assaults by investigating novel approaches and solutions. As the study progresses, a careful analysis of such link layer flaws and the suggested mitigation techniques will be essential to strengthening WLAN security posture and guaranteeing an infrastructure for communication that is both safe and skilled at fending off new threats.

II. RELATED WORKS

An extensive investigation of literature on 802.11 reveals that, rather than offering workable answers, the majority of current research focuses on comprehending the mechanics of DoS assaults. By utilizing the Advanced Encryption Standard (AES), the IEEE 802.11i standard improved wireless network security with Cipher Block Chaining Message Authentication Code Protocol (CCMP). But only data frames are shielded from this, leaving management frames exposed. With applications like WLAN-jack and Airjack, adversaries may simply counterfeit management frames, which results in deauthentication and dissociation framesthat are broadcast to all WLAN users, inflicting extensive disruption.

This study suggests an Integrated wireless connectivity Intrusion Detection and mitigation Mechanism to solve the major gap in link layer security. The system makes use of a cutting-edge Automated Wireless Attack Detection Algorithm (AWADA) which presents automation features for real-time mitigation in addition to detecting and classifying link layer threats. To be more precise, the system focuses on disassociation and deauthentication threats in an effort to protect wireless local area networks (WLANs) from interference that may disconnect authorized users. As stated in the introduction, this paper's main contribution is the conceptualizing and design of an advanced system to detect wireless link layer assaults that is intended to be used for network auditing, packet capture and analysis, and detection of such attacks. Strengthening the security and performance of Wireless

Local Area Networks (WLANs) is the main goal. Interestingly, the suggested system only runs in infrastructure mode and focuses on the different kinds of management frames, taking care of a crucial part of flaws at the link layer.

This article explores the body of knowledge that has been established in Section II and provides an extensive overview of relevant work in the field in the parts that follow. A brief introduction to wireless networks is given in Section III, laying the groundwork for Section IV's more in-depth examination of the link layer as well as associated several attack vectors. In Section V, the framework of the suggested system is discussed in detail, illuminating the subtleties of its functionality and design. In Section VI, the intricacies of the wireless connectivity layer assaults detection system's functioning are explained in depth. Particular attention is paid to the subtypes of management frames and the subtle ways in which the system operates inside the infrastructure mode. In result, Section VII provides a summary of the system's results and suggestions for improving WLAN performance and overall security. This methodical methodology guarantees an exhaustive and coherent investigation of the findings reported in this manuscript. Numerous research on wireless systems for detecting and preventing intrusions may be found in the field of network security. Even with these systems' advancements, there are still certain issues and shortcomings, especially with regard to the security of management frameworks in current WLAN architecture. One notable issue is the frequency of deauthentication attacks, which still represent a serious security risk because management frames are not protected.

James Yu and Chibiao Liu [4] made a significant contribution to this subject by introducing an experimental framework intended to identify and address attacks known as Association Request Flooding (AssRF) and Authentication Request Flooding (AuthRF). Their methodology includes TCP assaults as well as wireless voice over IP connections. As defenses against AuthRF and AssRF assaults, the researchers used Traffic Pattern Filtering (TPF) and MAC address filtering (MAF). Thuc Nguyen, Bao
N. Tran, and Duc H. M. Nguyen [1] advocated a mechanism using the Letter-Envelope Protocol for authorization management frames throughout the association process in order to prevent denial-of-service (DoS) attacks, specifically deauthentication anddisassociation attacks.

For disassociation DoS attacks, Baber Aslam, M Hasan Islam, and Shoab A. Khan [2] proposed a sequence number-based method. By employing a pseudo-random sequence number (based on PTK) for disassociation notifications, their technique offers a robust defense against successive disassociation attacks. For the purpose of detecting and preventing Media Access Control (MAC) layer Denial of Service (DoS) attacks, L. Arockiam and B. Vani [9,10,11] proposed a comprehensive framework with three novel MAC layer security algorithms: Intruder Detector and Manager (IDM), Letter Envelop Protocol with Traffic Pattern Filtering (LEPT), and MAC Spoof Detection and Prevention (MAC SDP DoS). When compared to current techniques, their suggested algorithms performed better in terms of reduced recovery times and packet resend rates. The framework in question is noteworthy for its cost-effectiveness and lack of firmware upgrades upon implementation in WLAN operational networks.

The work of Shahidan M. Abdullah, Haydar Imad Mohammed, and Haitham Ameen Noman adds to the conversation on automated detection procedures and represents a significant advancement in protecting wireless networks from deauthentication and disassociation assaults [6]. The development of the Python "IJAM" program demonstrates a dedication to security enhancement and emphasizes the significance of customisation in addressing particular vulnerabilities. The tool's usefulness and potential influence in real-world circumstances are demonstrated by its effective implementation on Linux systems. But the difficulty encountered with Windows OSs because of the restrictions on turning on monitor mode highlights how complex cross- platform compatibility is. Because operating systems are becoming more and more diverse, researchers and programmers are faced with the difficult task of developing adaptable solutions that work well in a variety of settings. This calls for a concentrated effort to develop detection strategies that go beyond the limitations of operating systems and provide a strong protection against assaults at the wireless connection layer on any platform. It is crucial to have detection technologies that are resilient and adaptive to various operating systems when developing comprehensive security solutions. The constraints faced by Windows environments act as a catalyst for the research sector to pursue novel approaches that will lead to the creation of automated detection techniques that are broadly applicable in the field of wireless network safety.

III. WIRELESS NETWORKS

Remember this Wireless networks—also known as wireless fidelity, or Wi-Fi—are extensively utilized in a range of contexts and are developed using the IEEE 802.11 standard protocol. This standard defines key protocol specifications for the wireless medium access control (MAC) and describes the link layer communication behavior between stations in a wireless network. This study focuses on wireless networks, which are made up of several Access Points (APs) and numerous stations, also known ascustomers [2].

Within the framework of this study, a wirelessly capable device—such as laptops or PDAs having a wireless networking interface—is referred to as a client. The security features of these wireless networks are particularly addressed by the Integrated Wireless Intrusion Detection and mitigation System. Through wireless local area networks (WLANs), Wi-Fi access points (APs) operate as base stations or servers. They use Beacon Frames, which carry the Service Set Identifier (SSID) data, to periodically announce their existence and capabilities [10]. The AP is uniquely identified by a character string called the SSID. In accordance with this SSID signal, authenticated client devices inside the AP's coverage area can identify and choose to join the network.

It is important to remember that although WLANs use the unlicensed 2.4 and 5 GHz spectrum for communication, the main focus of this research is on the creation and deployment of an automated system meant to identify and address possible security risks inside these wireless networks. The purpose of this Integrated Wireless Intrusion Detection and Mitigation Program is to improve Wi-Fi network security posture by automatically detecting malicious activity, blocking unauthorized access, and quickly

reacting to any threats. The design, implementation, and salient characteristics of this novel system will be thoroughly examined in the next sections to offer a thorough grasp of its function in defending wireless networks against cyberattacks.

A. Operating Modes

Wireless networks, sometimes referred to as Wireless Fidelity (Wi-Fi), have two primary operating modes, following the 802.11 networks standard. Ad-hoc mode refers to the first alternative, where individual stations (STAs) connect to one another directly without requiring an access point (AP). Every STA in the network is supported by an exclusive access point (AP) in the second mode, which is referred to as infrastructure mode. The majority of 802.11 networks function in infrastructure mode, which is managed and orchestrated by an access point (AP). The infrastructure mode, which is essential to wireless local area networks, depends on the existence of Access Points (APs), which act as hubs linking different network stations. Regarding our Integrated Wireless Intrusion Detection and Mitigation Program that we are proposing, priority positioned in WLAN transmission on the network's infrastructure.

TABLE 1 Secure Wireless Configurations

OPERATING MODE	SECURITY LEVEL
Open System	No authentication or encryption
WEP	Basic encryption, vulnerable
WPA	Improved security, dynamic keys
WPA2	Strong encryption, recommended
WPA3	Latest and more secure
Enterprise Mode	Centralized user authentication
Personal Mode	Simplified security

The Integrated Wireless Intrusion Detection and Mitigation System is intended only for use in infrastructure wireless local area networks. This intentional decision is in line with the widely used method of operation in many Wi-Fi networks, in which an access point controls communication in a centralized manner, providing an ideal setting for putting strong security measures in place. The following sections will go into more detail about how the system uses infrastructure WLAN properties to its advantage in order to detect and neutralize any wireless security threats.

B. Management Frames

The Medium Access Control (MAC) layer, and a crucial component where information is organized and transferred in frames, manages data transmission in Wi-Fi networks. The IEEE 802.11 protocol carefully classifies different types of MAC frames, focusing especially on management frames. To strengthen wireless networks' security framework, the Integrated Wireless Intrusion Detection and Mitigation System interacts closely with these management frames.

Three different message types are used in the IEEE 802. 11 Medium Access Control (MAC) layer communication: control, data, and management frames. Of these, management frames are particularly noteworthy since they play a crucial part in facilitating clients' easy integration with the wireless network's infrastructure via an access point (AP) and continuous communication line.

Management frames serve more purposes than only association; they are essential to the creation and continued upkeep of a wireless network. These frames provide smooth data flow by fostering an ongoing communication link amongst wireless clients and APs. Within the framework of 802.11 administrative frames, Frames Command, Time frame, and Destination Address (DA) are among the crucial pieces of information contained in a conventional 24-byte header. The main objective of the Integrated Wireless Intrusion Detection and Mitigation System is to improve the security posture of wireless networks. In this situation, it is crucial to comprehend the nuances of managerial frameworks. The subsequent sections of this discourse will intricately elaborate on how the system intelligently leverages the information encapsulated in management frames. The following portions of this talk will go into great detail about how the system makes use of the data that is included in management frames. Through the autonomous detection and mitigation of possible security concerns, this intelligent use seeks to strengthen the resilience of the wireless connection against malicious activities and unauthorized access. A detailed examination of the system's methods and contributions to safeguarding the ever-changing wireless communications environment will be provided soon.

Source address (SA), BSSID, Sequence control and Frame Check Sequence (FCS).

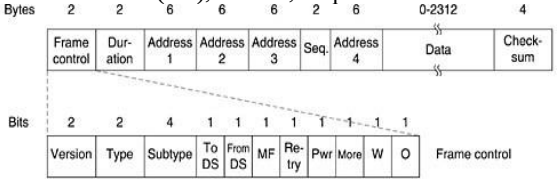

Fig. 1. IEEE 802.11 MAC management frame

IV. LINK LAYER

The Data transit among network elements is greatly aided by the link layer, commonly referred to as layer 2 [9]. The IEEE 802.11 LAN standards describe two essential sublayers inside the link layer, namely Medium Access Control (MAC) and Logical Link Control (LLC). The MAC layer is covered in this section along with its functions, composition, and susceptibility to many forms of assaults.

A. Medium Access Control (MAC) Layer Overview

The network's physical layer and LLC sub-layer are connected by the MAC sub-layer, which is categorized as the fundamental link layer (layer 2) in the OSI seven-layer design. It manages the data packet exchange across Network Interface Cards (NICs) over a shared channel. The assignment of distinct identifiers, or MAC addresses, defines the MAC layer. The 48 bits (12 hexadecimal digits) that make up MAC addresses serve as unique layer 2 addresses. They are utilized in several network technologies, including as Ethernet, and are crucial to IEEE 802.11 network technologies.

B. Types of Attacks on the Medium Access Control (MAC) Layer

The Integrated Wireless Intrusion Detection and Mitigation System is a MAC layer defense mechanism that targets and neutralizes particular attack patterns. Denial-of-service (DoS) attacks at the MAC layer specifically take advantage of the unencrypted transfer of management frames that contain source MAC addresses. Competitors use easily accessible technologies to launch DoS attacks at the MAC layer against Access Points (APs) or clients.

In MAC layer denial-of-service attacks, communications sent across clients and APs are spoofed. Spoofing frames to the receiver, attackers change the MAC address of the client or the AP. When the recipient processes these frames without knowing they are legitimate, there might be security lapses. The Integrated Wireless Intrusion Detection and Mitigation System guards against a variety of MAC layer threats, such as masquerading, deauthentication flooding, disassociation flooding, resource depletion, flooding of probing requests, authentication flooding, and association flooding..

C. Masquerading Denial-of-Service (DoS) Attacks

Malicious MAC address spoofing of verified Access Points (APs) or authorized client MAC addresses is the basis for masquerading denial-of-service (DoS) attacks. By addressing certain masquerade attack forms, the Integrated Wireless Attack Detection and Mitigation System aims to mitigate their effects.

a) 1) Disassociation Offensive

A client and an AP send an association message after authentication to create the client's affiliation with the AP. A bogus message is sent to the AP by the attacker in a disassociation attack. The AP responds to this communication by disassociating the client whose MAC address appears in the message falsely. A denial-of-service situation results from this disassociation, which breaks the contractual relationship amongst the client and the AP.

b) Deauthentication Attack

One kind of masquerade DoS attack that exploits interactions between an end user and a wireless access point (AP) is the deauthentication attack [6]. An important stage in creating an encrypted connection with a wireless access point is the four-way handshake, which this attack seeks to prevent the client from completing. The assault has two primary forms:

c) Targeting Specific Stations or Clients:

The attacker concentrates on interfering with certain customers' or stations' communication within the wireless connection. The attacker stops the target client from finishing the handshake procedure and obstructs its ability to connect to the AP by delivering misleading deauthentication packets.

d) Attacking the Target Access Point:

2) In this version, the attacker targets the target access point with deauthentication messages. The attacker tries to thwart the four-way handshake that clients begin when they try to establish a connection to the designated access point by altering the MAC address information.

D. Denial-of-Service Attacks

Attacks known as resource exhaustion seek to exhaust system resources, such as memory and processing power [6]. When these assaults go unchecked, they cause the denial of services that were originally meant for clients who were legitimate. The Automated Wireless Attack Detection and Mitigation System is designed to defend against Resource Exhaustion assaults,

including those that use Examine Request Flood, Authentication Request Flood, and Association Request Flood in the context of MAC layer Denial-of-Service (DoS) attacks.

1) Attack of Probing Request Flooding

Access Points (APs) usually reply to a client's probe request by supplying details concerning their wireless network in order for the customer to connect and verify. An intruder assaults access points (APs) by transmitting an excessive number of investigate demands, each with a fictitious MAC address. This technique is known as probe request flooding. Probe-request flooding [4] is a flooding technique designed to interfere with APs' regular operations, making it more difficult for them to reply to valid clients and perhaps resulting in service denial.

2) Association/Authentication Flooding Attack

An attacker uses MAC address spoofing to start association and authentication attempts with a particular access point during an association/authentication flooding exploit [4]. The main goal of the attack is to completely fill the memory and processing capabilities of the targeted access point by continuously flooding it with association or authentication requests. As a result, connected clients encounter reduced or completely interrupted connectivity, which has an impact on their connection state.

The System uses sophisticated techniques to recognize and thwart denial-of-service (DoS) assaults including resource exhaustion. By doing this, the system hopes to protect wireless network functionality and the availability, guaranteeing uninterrupted delivery of services to customers that are authentic. The parts that follow will go into more detail on the tactics and safeguards the system put in place to successfully lessen these

Resource Exhaustion DoS attacks at the MAC layer.

V. ARCHITECTURE OF PROPOSED SYSTE

This section describes the envisioned system's architecture. The suggested system architecture comprises an Access Point (AP), a victim station (STA), a monitoring machine, a genuine machine, and an attacker station (STA). To obtain all of the received and transmitted frames from AP, the monitoring device connects to AP. The WLAN interface is divided into two modes. While the others operate in controlled (stations) capacity for investigating a STA, one operates in surveillance mode to record frames. It is possible for an attacker to pose as the victim STA or the AP. Ultimately, an alert will appear on the screen along with a detection notice.

TABLE 2 Network Components

COMPONENT	FUNCTIONALITY
Access point (AP)	Wireless connectivity hub oversees and makes connecting with other stations easier.
Attacker Station (STA)	acts in a malevolent manner creates and sends maliciously intended frames.
Victim Station(STA)	stands for the intended gadget. Attacker Station assaults are a possibility.
MonitoringMachine	oversees the operations of the network records both inbound and outgoing frames creates an interface with the AP.
LegitimateMachine	behaves inside the network as a benign entity.

VI. A PROPOSED SYSTEM FOR DETECTING WIRELESS LINK LAYER ATTACKS

The Python-written Wireless Link Layer Attacks Detection System (WLLADS) operates in a Linux environment. Its purpose is to gather every bit of Wi-Fi data and to identify and stop wireless intrusion. The attacked packets are automatically saved into a file by this system, which operates in real time. The following applications are needed to run this proposed system: Wireshark, Aircrack-ng suite, Python 2.7, Root access (Admin), Xterm (Terminal emulator that runs at once on the same display), Mergecap (Integrate a number of saved captivated files into one), and Wireless interface that is suited of keeping track and injection. Backtrack and Kali-Linux already come with certain pre-installed programs.

A. Algorithm for Detecting Attacks at the Wireless Link Layer

The Wireless Link Layer Attacks Detection Algorithm (WLLADA), a suggested algorithm, is described in this article. This method detects wireless intrusion, checks network penetrations, and stops stations from connecting to access points in WLAN architectural mode. The proposed method works in a Linux environment.

Algorithm: WLLADA (Wireless Link Layer Attacks Detection Algorithm)

1. Initialize:
   - Set a threshold for the frequency of disassociation attacks.
   - Create a data structure to store recent MAC addresses and their associations.
   - Define a time window for tracking recent events.
2. Monitor Network Traffic:
   - Continuously capture and analyze wireless network traffic.
   - Extract MAC addresses, frame types, and timestamps from management frames.
3. Detect Anomalies in MAC Addresses:
   - For each received management frame:
   - Check if the source MAC address is within the expected range or known list.
   - If not, flag it as a potential anomaly.
4. Track Association and Disassociation Events:
   - Identify association and disassociation events in management frames.
   - Maintain a record of recently associated MAC addresses.
   - Detect disassociation attacks:

- If a disassociation event is detected:
- Check the frequency of disassociation events within the defined time window.
- If it exceeds the threshold, flag it as a potential disassociation attack.

5. Update Data Structures:

- Regularly update the data structures:
- Purge outdated entries from the MAC address tracking list.
- Adjust counters and timestamps for association and disassociation events.

6. Alert Generation:

- If anomalies in MAC addresses or potential disassociation attacks are detected:
- Generate alerts or log entries indicating suspicious activity.
- Include relevant information such as MAC addresses, timestamps, and the nature of the detected anomaly.

7. Response Mechanism (Optional):

- Implement a response mechanism based on the severity of the detected attack.
- Examples of responses include logging, blocking, or notifying network administrators.

8. Repeat:

- Continuously repeat steps 2-7 to monitor and analyse network traffic in real-time.

B. Detection Mechanism

The Automation of Wireless Link Layer Offensive system's detection technique makes use of fingerprinting, a procedure designed to produce distinct profiles for different workstations according to their particular attributes. By comparing endpoint profiles to the present configuration of workstations in the wireless connection, the network equipment is able to determine workstations thanks to profiling. In order to create a thorough profile, the procedure entails gathering specific data on every workstation, such as NIC drivers, software settings, and various driver workstations. The process of fingerprinting involves examining the timing patterns of different 802.11 administrative frames. Both passive and aggressive modes of application are possible with this approach. Using a sniffer to intercept data transmitted from a machine, passive fingerprinting entails tracing the intercepted traffic back to connected hosts on the local network. However, active fingerprinting is a flexible tool that can beused by both administrators and possible attackers to do tasks including finding open ports on distant servers, assessing packet

filtering, finding live hosts, and figuring out the OS system. These fingerprinting techniques are used by the Automation of Wireless Link Layer Attack system to intelligently identify and neutralize such attacks, guaranteeing strong wireless network security.

C. Implementation and attack types

A bespoke test network consisting of a single access point (AP), an end-user PC, an intruder's notebook, and a device for tracking was set up for real-world assessment. A key part was performed by the Linux program Aircrack-ng, which used its dumping and surveillance modes to create deauthentication packets and aid in the breaking of the wireless network's encryption [1]. Especially useful for spoofing and sending deauthentication packets to be related clients of a certain access point was the utility's aireplay-ng tool.

The Airodump-ng utility was used to quickly locate, and scan related clients connected to a specified access point. Its features expedited the procedure by providing a thorough overview of related customers and facilitating the planning of focused deauthentication assaults. This safe testing ground provided an essential foundation for methodical attack examination, offering insightful information on the complexities of the Wireless Link Layer Intrusion Prevention System.

VII. CONCLUSION

Denial-of-Service (DoS) attacks can more easily target the Link Layer due to the transparency of unencrypted administration frames. This is due to the fact that wireless connection layer attacks are more likely to target exposed source MAC addresses. In response to this concern, a comprehensive technique for detecting and preventing wireless connection layer attacks has been released. The proposed Wireless Link Layer Attacks Detection Algorithm (WLLADA) is a Linux-based system that uses commands such as iwlist and airodump-ng to monitor network information, record and analyze surrounding traffic, and analyze key parameters like the number of unsavoury pieces of information, station/Access Point MAC addresses, and captured and evaluated data packets.

When deployed in a real-time configuration, this solution helps Wireless Local Area Networks (WLANs) improve both performance and security at the same time. The detection and reduction of wireless link layer assaults is the primary focus, which creates a strong defensive mechanism against any incursions. Nonetheless, it is critical to recognize how security risks are always changing. To strengthen the entire security posture of WLANs, the study will expand in the future to include preventative and auditing modules designed specifically for management frames. This proactive strategy ensures that the suggested system is robust and adaptive in the face of new threats, in line given the constantly changing dynamics of cybersecurity.

REFERENCE

[1] J. Bellardo and S. Savage, “802.11 Denial of Service Attacks Real Vulnerability and Practical Solutions", proceeding of the12th USENIX Security Symposium, pp. 15-28, 2003.

[2] Aircrack-ng official website http://www.aircrack-ng.org.

[3] G. Raju and R. Akbani, "Authentication in wireless networks", Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci., Jan. 2007.

[4] K. J. Hole, E. Dyrnes and P. Thorsheim, "Securing Wi-Fi networks", Computer, vol. 38, no. 7, pp. 28-34, Jul. 2005.

[5] A. Dorri, S. R. Kamel and E. Kheyrkhah, "Security challenges in mobile ad hoc networks: A survey", Int. J. Comput. Sci. Eng.Survey, vol. 6, no. 1, pp. 15-29, 2015.

[6] R. Meddeb, B. Triki, F. Jemili and O. Korbaa, "A survey of attacks in mobile ad hoc networks", Proc. Int. Conf. Eng. MIS (ICEMIS), pp. 1-7, May 2017.
[7] J. M. De-Fuentes, A. I. Gonzalez-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks" in Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, Hershey, PA, USA: IGI Global, 2011.
[8] H. Hasrouny, A. Samhat, C. Bassil and A. Laouiti, "VANet security challenges and solutions: A survey", Veh. Commun., vol. 7,pp. 7-20, 2017.
[9] Sheikh, Liang and Wang, "A survey of security services attacks and applications for vehicular ad hoc networks (VANETs)",Sensors, vol. 19, no. 16, pp. 3589, 2019.
[10] A. Raoof, A. Matrawy and C.-H. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things", IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1582-1606, 2nd Quart. 2019.
[11] S. Wang and T. Jin, "Wireless network-on-chip: A survey", *J. Eng*., vol. 2014, no. 3, pp. 98-104, 2014
[12] Kavousi-Fard, A.; Su, W.; Jin, T. A machine-learning-based cyber-attack detection model for wireless sensor networks inmicrogrids. *IEEE Trans. Ind. Inform.* **2020**, *17*, 650–658.
[13] E. Tews and M. Beck, “Practical attacks against WEP and WPA,” in *Proceedings of the 2nd ACM Conference on Wireless NetworkSecurity (WiSec '09)*, pp. 79–85, March 2009.
[14] M.-K. Choi, R. J. Robles, C.-H. Hong, and T.-H. Kim, “Wireless network security: vulnerabilities, threats andcountermeasures,” *International Journal of Multimedia and Ubiquitous Engineering*, vol. 3, no. 3, pp. 77–86, 2008.