Infiltrations into Wireless Networks by Attackers

Haroon Rashid Hammood Al Dallal
Bachelor's degree, Department Engineering in Communication Techniques, Al-Furat Al-Awsat Technical University, Najaf, Iraq.
Master's degree, Department Infocommunication Technologies and Communication Systems, Saratov State Technical University, Saratov, Russia.
haroonra1994@gmail.com

Yasir Adil Mukhlif
Bachelor's degree in Computer Engineering Technology, Al-Ma'aref University College, Al Anbar, Iraq.
Master's degree, Department Electrical and Computer Engineering, Altınbaş University, Istanbul, Turkey.
yasradl071@gmail.com

ABSTRACT

Due to the insecurity of wireless channels, communications are open to a wide variety of different sorts of assaults. It is still difficult and important to solve the problem of communications in wireless networks. In this study, current developments It presents the requirements and capabilities necessary for encrypting data carried out via "wireless networks". "Wireless networks" are now being utilized in a broad variety of commercial and military applications to collect data in real-time and dependent on occurrences. The nature of network deployment renders them susceptible to a variety of security risks. Traditional security techniques are insufficient to ensure the safety of the nodes because of the constraints placed on available resources. The study of many aspects of network security has led to the development of several preventative measures. Throughout this article, we have looked at several security techniques. We created and analyzed strong model for the integration of heterogeneous wireless networks by using different security techniques in terms of the overheads associated with the packets and compared the amount of time it took to send the packets, the average amount of delay, and the amount of energy used. That result shows that the transmission outgoings were reduced as compared to other techniques, and this is demonstrated by the reduced costs.

Keywords:

I. Introduction

Wireless networks can capture and transmit data from areas that are inaccessible to traditional networks for a variety of reasons, including those related to the environment and military strategy. In order to provide mobile users with adaptable and flexible cellular networking, wireless networking is becoming more and more common among the much more stimulating designs for wireless systems that can build themselves and organize connectivity. One of the most promising opportunities for offering wireless access to mobile consumers is wireless networking. This concept may be used for several wireless access technologies, such as wireless personal area networks (WPAN), wireless metropolitan area networks (WMAN), and wireless local area networks (WLAN). The presented research [1] predicts that WMNs will be able to

outperform mobile ad hoc networks, WLANs, WPANs, and wireless local area networks overall while also overcoming their limitations. Wireless networks are more susceptible to security risks than wired ones because of the computational and power constraints they face. The addition of expensive security measures presents considerable hurdles in terms of compute power, memory limitations, and energy consumption when trying to create a lightweight security system that can protect wireless networks from being attacked. Because A hacker can intercept network traffic without physically being in the same building as the network. Because wireless networks communicate by WLAN waves, a hacker from a nearby place may simply sniff the network. To locate the SSID and breach a wireless network. Once a hacker has gained access to your system, they can install a keystroke logger to record every username and password typed, impersonate your email by sending harmful links and malware to your contacts, and copy network traffic, including card transactions including bank account login details.

As shown bellow in the figure, there are following access points and extension in the wireless network;

Figure 1; showing wireless access points.

II. Wireless Security Overview

Since WLANs are often implemented as an addition to fixed or connected LANs that already exist, it is required to increase the security of "WLANs" to levels that are closer to or something equal to the protection of wired-up "LANs". This is because WLANs are different from their cable counterparts in nature. As a general rule, "IEEE" 802.11 may be utilized in two modes, referred to as "Ad hoc and Infrastructure modes," for two different types of network topologies. A wireless local area network (WLAN) is the setup of wireless stations (STAs) connecting electronically to a network access point (AP) that is connected to the conventional wired connection in the infrastructure architecture. Before a connection can be made between an STA and an AP, three steps must be finished: (probing, authentication, and association) [2]. The STA has two choices at the time of the probe: it can actively apply to join an AP or it may passively monitor for AP signals and attempt to automatically sign up with them. The next phase is termed verification, and it is during this phase that the AP will confirm the identity of the STA by using a variety of authentication techniques, some of which will be covered in greater detail further on in this publication. The STA will request the association with the AP after fully verifying itself. If the request is approved, the AP will add that STA and the wireless devices that are associated with its database. An AP can have several STAs associated with it, but an STA can only have one AP associated with it at a time. The three phases of WLANs are illustrated in Figure 1.

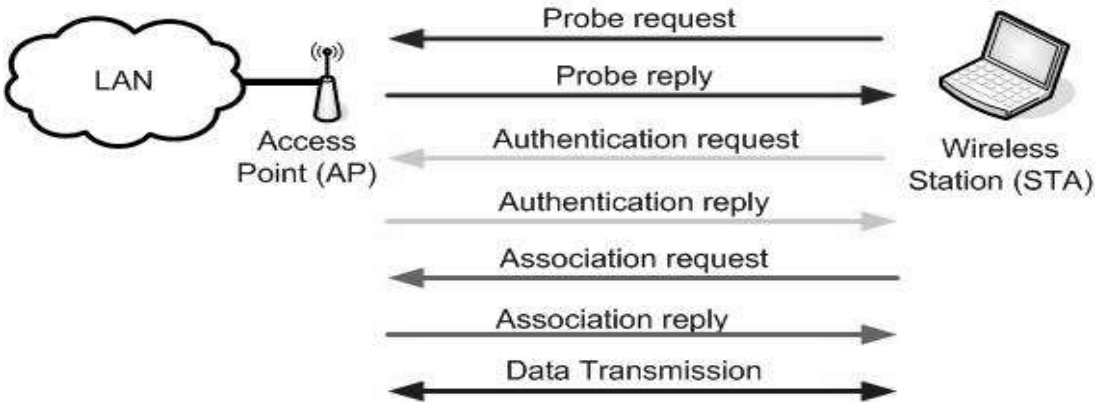

Figure 2 depicts the three stages that must be traversed by WLAN in order to successfully establish connections between access points and STAs. These include questioning, proving one's identity, and forming associations.

The protection of the wired local area network (LAN) will ultimately be compromised as well if the protection provided by the wireless local area network (WLAN) is breached in any manner. Wireless local area networks (WLANs) raise a number of security issues, including the use of "radio frequency (RF)" as a data transmission medium and the fact that each communication is broadcast to every site that is within the WLAN's service area. [2], [3]. There is significant possibility of eavesdropping and man-in-the-middle attacks [4] since the spread of airwaves cannot be stopped or confined to a single room. In wired networks LANs, the situation is different since significant servers may be protected in a separate room and data flow happens across a cable that can be monitored and subject to some level of control. As a result, wireless LANs are less secure than traditional LANs. Three separate security objectives must be kept in mind while dealing with utilizing wireless local area networks (WLANs): WLAN authentication, data transmission secrecy, and data transmission integrity [5]. A solution that would enable STAs to verify themselves before being permitted access to the WLAN must be put in place immediately in terms of authentication. High degrees of effectiveness, adaptability, and reliability is needed for these methods. In order to guarantee secrecy throughout the information transmission process between STAs and AP, extremely sensitive data should be covered.

III. Concerns Related To Network Security

All of the devices that are covered by the access point service have access to any information in the form of being transmitted either toward or away from the entry point. Even while functionality makes it simple to connect to a wireless network, it leaves the system vulnerable to several security flaws. When compared to wired networks, wireless networks place a significantly greater emphasis on and are required to comply with, stringent security measures. This might be explained by the fact that the information was sent to the communities via a "wireless network." Additional safety measures must be taken when transferring confidential data through a wireless network, such as by financial companies, banking systems, military systems, information on terrorists, and so forth [6,7]. Attacks made against wireless networks may be divided into two primary categories: passive and aggressive, with the distinction between the two based on how they disrupt communication. Attacks made on wireless networks are shown in figure 3.

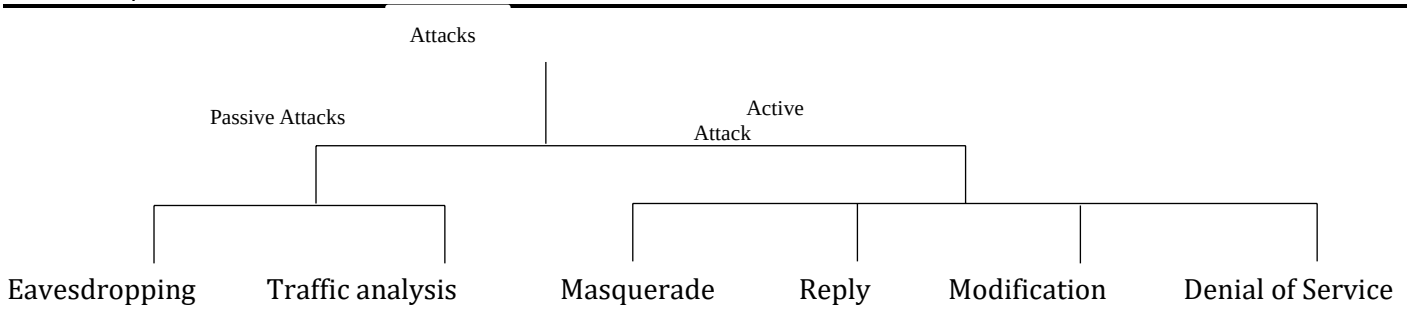

Fig. 3. The Various Methods of Attacking Wireless Networks

The information that is being communicated through the network may be obtained via the use of a passive assault, which does not disrupt the transmission. whereas an active assault disturbs the usual operation of the network, which indicates that it may stop communication, manipulate information, or even manufacture it [8, 9, 10].

Passive attacks: Passive attacks eavesdrop or spoof about the information, and The aggressor makes an effort to get unauthorized access to the data that is now being transferred to steal it. There are two distinct types of passive assaults, and they are as follows:

- **Eavesdropping:** Is a kind of assault in which the perpetrator makes an effort to read the contents of an email or a file that is in the process of being transmitted.

- **Traffic analysis:** The perpetrator of this type of attack is the victim ,attempts to reveal the localization and identification of nodes that are related by analyzing the flow of traffic. In addition to this, the attacker is able to keep track of the length of the messages that are being transmitted as well as the frequency with which they are being transmitted. These are both significant bits of data that can be used to formulate educated guesses regarding the nature of the information that is being communicated.

Active attacks: these assaults may be broken down into the following four categories:

- **Masquerade :** In this style of attack, an entity pretends to be an authorised entity in order to get access to certain information or to achieve further permissions. This type of assault has the potential to be highly hazardous.
- **Reply :** In this type of assault, the data is captured without the user's active participation, and then it is maliciously repeated or delayed in a manner that is dishonest, fraudulent, or dishonest.

- **Modification:** In these kinds of assaults, the hacker will try to delay or swap the communications.

- **Denial of Service:** This kind of attack occurs when an adversary prevents authorized preventing users from accessing particular services or other kinds of "IT resources"

IV. Developing An Ideal Security System

Enterprises should methodically prepare and implement a coordinated strategy to secure their wireless network against loss of data and illegal access. While the ultimate security solutions depend on the amount of protection necessary and available money, there are certain essential suggestions and approaches to become started. When designing the perfect surveillance system, four aspects need to be taken into account first and foremost. The following are some examples of characteristics [7, 9]:

Firewall:
Using a firewall in a wireless network establishes a strong security foundation to prevent unauthorized access and provide secure network access for your on-site and remote staff, business associates, and customers. Firewalls are an essential security component in all secure networking systems, including wired and wireless networks.

Authenticity: Is the process of distinguishing authorized users from unauthorized ones. Authenticity refers to this process. The verification of the identification of each node in the network may be used to accomplish this. Any two nodes in a wireless network that are communicating with each other must first check and validate their identities [7].

Confidentiality: The only people who should be able to access the wireless network are the ones who have been permitted to do so. Unauthorized users should be prevented from gaining access to the wireless network and from disclosing the information. The sort of access that a user has is determined by the privileges that they have been granted, such as reading only, printing, or knowing whether or not the object may be accessed [7].

Integrity: Is the state of maintaining the information's correctness and dependability while it is being sent across a wireless network, and is referred to as "the integrity." Because of this, the information must never be altered while it is being stored. Modification operations, such as the addition, deletion, or replacement of data, may only be carried out on transmitted information by users who have been specifically granted permission to do so.

Availability: Because of this feature, it can be deduced that the wireless network is, in fact, accessible to the authorized users who want to use it, provided that they make the appropriate arrangements. A denial of service is the opposite of an available service, and it has the effect of preventing authorized users from connecting to a wireless network. Therefore, the user will not have a positive experience [7, 9].

V .Assessment Of Components Of Security Requirements

There is no such thing as free security. When additional security features are added to a network, the network experiences an increase in both its overall level of security as well as an accompanying increase in the amount of communication, processing, and administrative overhead. Therefore, in a resource-constrained ad hoc network, network performance becomes a significant consideration. This pertains to aspects of the security solutions such as their scalability, robustness , and service availability, among other things. However, the topic of how well their solutions perform in terms of network performance is typically disregarded. This is despite the fact that the focus in many recent ideas is placed on how strong the cryptographic security of the solutions they offer. Network performance and security strength are two factors that are equally important, and one of the primary obstacles that must be overcome when building security for wireless networks is to locate a happy medium between the two extremes. Figure 3 illustrates the many aspects of a wireless network's security that need to be addressed in order to fulfil the necessary standards. [11]

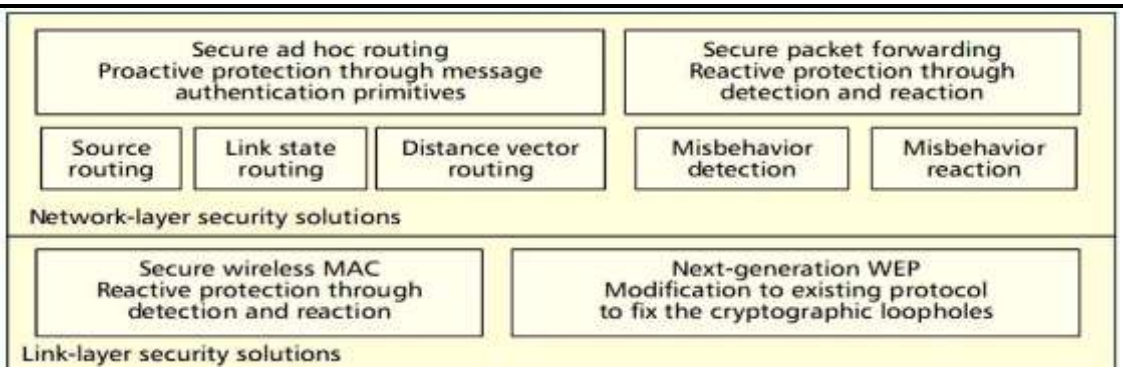

Figure 4. Components of the Safety and Assurance Option

More sophisticated and subtle hazards will continue to be the focus of ongoing research efforts. The enemy may, for example, continue to destabilise existing network nodes, or they could construct their own identity to mimic another approved node [12]. In order to generate a wormhole [13], two attacker nodes must collaborate in order to create a bypass for the normal flows between them. in relation to "on-demand ad-hoc "network systems, It is possible for the attackers to target the normal maintenance of the route and then advertise that a functioning link has been interrupted [14]

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Figure 4 . Illustrates how security solutions for wireless networks should offer comprehensive protection that extends throughout the entirety of the protocol stack.

The fact that they use an open peer-to-peer architecture is the root cause of their primary security flaw. Each mobile node in a wireless network has the potential to act as an intermediary and relay transmissions of data intended for the network's other nodes. This is in contrast to wired networks, which have dedicated routers. The wireless channel can be accessed by both authorized users of the network and unauthorized hackers who are trying to breach the security of the network. As a consequence of this, there is not a distinct line of defense present in it from the point of view of the design of the security system. The line that delineates the internal network from the rest of the world on the outside gets increasingly unclear. It is not the case clearly specified architecture in which even just one security solution may be implemented might be installed, so we cannot implement any of them.

V I . Conclusion

In summary, the most essential security needs for the wireless network have been looked at and evaluated. When attempting to come up with solutions for the security issues that the wireless network has, these criteria should be used as a general notion. This article briefly discusses the

security-related features of a variety of wireless network types, including cellular networks, wireless mesh networks, ad hoc networks, sensor networks, WLANs, and others. The next step is to create a model for the integration of heterogeneous wireless networks that clarifies and takes into account those security reference points that are situated at the boundaries of several "networks" of a particular type. Concerns regarding open wireless design can be resolved, as problems in adopting a model for network integration, which provides a framework that can be used to address the stated concerns. In addition, numerous forms of security attacks are outlined, the bulk of which affect wireless networks..

References

1. Ian F. Akyildiz, Xudong Wang and Weilin Wang, "wireless mesh networks: a survey," Computer Networks, vol. 47, pp. 445-487, Jan. 2005.
2. IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).
3. Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.
4. Wang Shunman, TaoRan, WmgYue and ZhangJi, "Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.
5. Matthew S. Gast, 802.11 Wireless Networks, O'REILLY, 2002.
6. Kevin Tyrrell. 2003. An Overview Of Wireless Security Issues. SANS Institute.
7. NASEER AHMAD. July 2009. Security Issues in Wireless Systems. thesis is presented as part of the Degree of Masters in Electrical Engineering with emphasis on Telecommunications. Blekinge Institute of Technology.
8. Teodor-Grigore Lupu. 2009. Main Types of Attacks in Wireless Sensor Networks. Main Types of Attacks in Wireless Sensor Networks. ISSN: 1790-5109. ISBN: 978-960-474-114-4.
9. Yulong Zou. Jia Zhu, Xianbin Wang, and Lajos Hanzo. September 2016. A Survey on Wireless Security: Technical Challenges. Recent Advances and Future Trends. Vol. 104. No. 9.
10. Shilpa Pareek, Ashutosh Gautam and Ratul Dey. April 2017. Different Type Network Security Threats and Solutions. A Review. International Journal of Computer Science (IIJCS). Volume 5. Issue 4.
11. D.Liu and P.Neng,"Establishing Pair wise Keys in Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS'03),2003.
12. B. Dahill et al., "A Secure Protocol for Ad Hoc Networks," IEEE ICNP, 2002
13. Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," IEEE INFOCOM, 2002.
14. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,"ACM MOBICOM, 2002.