www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 02, February 2023, pp : 106-110

e-ISSN : 2583-1062

Impact Factor : 5.725

A STUDY OF DIFFERENT TECHNIQUES USED FOR SECURE WIRELESS LOCAL AREA NETWORKS

Shubhi Danpati[1], Mr. Shailesh Khaparkar[2]

[1]M.Tech., Student, GGITS, Jabalpur, India.

[2]Associate Professor, GGITS, Jabalpur, India.

ABSTRACT

Wireless Local Area Networks (WLANs) are cost-effective and desirable gateways to mobile computing. They allow computers to be mobile, cable and communicate with speeds close to the speeds of wired LANs. These features came with an expensive price to pay in areas of security of the network. This work identifies and summarizes these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The work overviews both physical and logical WLAN security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man-in-the-middle attacks and Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs. However, WEP suffered many problems which were partially solved by the IEEE802.1x protocol. Towards perfection in securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of the security problems found in WEP and other temporary WLANs security solutions. This work reviews all security solutions starting from WEP to IEEE802.11i and discusses the strength and weaknesses of these solutions.

Keywords: Wireless Local Area Networks, WEP: Wired Equivalent Privacy, Temporal Key Integrity Protocol, Kerberos extensible authentication protocol, DoS: Denial of Service, LAN.

1. INTRODUCTION

Access to wireless networks at acceptable data rates was made possible by wireless local area networks (WLANs). For data communications in a wireless environment, the Institute of Electrical and Electronics Engineering (IEEE) has established standards and specifications. The driving technology standard forelands is IEEE802.11 [1]. Because WLANs are used as an extension of the existing fixed/wired LANs, it is important to raise their security to levels comparable to or higher than those of wired LANs because of their distinct nature. In general, IEEE802.11 can function in either the Ad hoc or Infrastructure network topology modes. The infrastructure mode of WLANs is the subject of this paper. A wireless local area network (WLAN) is created when wireless stations (STAs) communicate wirelessly with a network access point (AP) that is connected to the wired network. There are three stages involved in the creation of connections between AP and STAs: association, authentication, and probing [1]. During the probing phase, the STA can either actively request to join an AP or listen passively to AP signals and attempt to join the AP automatically. The authentication phase follows, during which the AP authenticates the STA using one or more of the authentication mechanisms that are discussed further in the paper. The STA will submit an association request to the AP following successful authentication; if the request is granted, the AP will include the STA in its list of associated wireless devices. An STA can only be associated with one AP at a time, whereas the AP can associate with multiple STAs. The three phases of WLANs are depicted in Figure 1.

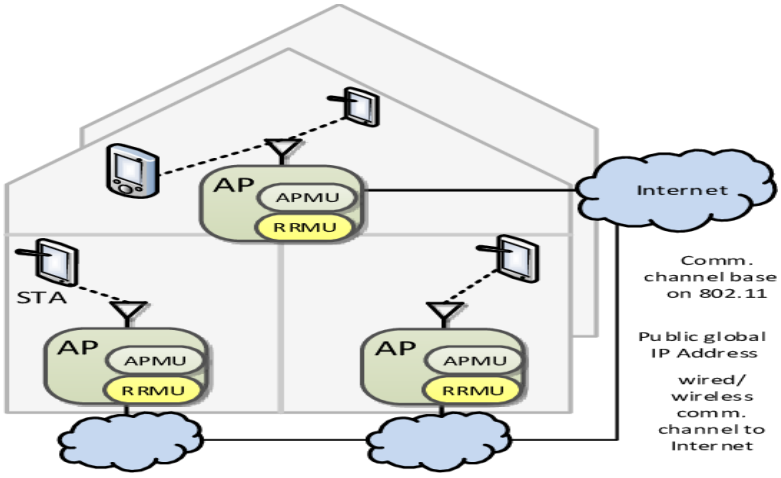

Fig. 1 The three phases underwent WLAN for the establishment of connections between STAs and AP.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 02, February 2023, pp : 106-110

e-ISSN : 2583-1062

Impact Factor : 5.725

These are probing authentication and association. A breach of the WLAN's security will eventually compromise the wired LAN's security. The use of radiofrequency (RF) as a medium for transmitting information and the fact that all messages are broadcasted to wherever the coverage of that WLAN can reach are just two of the many security concerns associated with WLANs [1]-[2]. Because airwaves cannot be blocked or locked in a room, there is a significant risk of eavesdropping and Man-in-the-middle attacks [3]. In wired LANs, critical servers can be isolated in a separate room, and data transmission is carried out by cables that can be partially monitored and controlled. Authentication of the WLAN, confidentiality and the integrity of the transmitted data are the three security objectives to keep in mind when working with WLANs [4]. To grant access to the WLAN, a mechanism that allows STAs to authenticate must be implemented in terms of authentication. These systems must be effective, scalable, and dependable. When information is transmitted between STAs and AP, the term "confidentiality" refers to hiding highly sensitive data. This is done to prevent other users from hearing the message. Maintaining the correctness and accuracy of information exchanged between STAs and AP is considered integrity [5]. These three objectives should all be met by any security solution. As more APs are added to the network, security and management issue becomes increasingly significant. As a result, methods to combat security threats must be developed as well as methods to centralize and manage security issues in both large and small WLANs. It is necessary to ensure the security of WLAN applications like wireless Internet and wireless e-commerce given their rapid spread. To address WLAN security issues, numerous papers have been written (see [3], [5]–[7] and [2]). The physical and logical aspects of the WLAN security issue are examined in this paper, along with the currently available solutions. As a result, the major threats to the security of WLANs as well as the available security protocols and technologies will be discussed in the following sections.

2. LITERATURE WORK

Using only colour and depth images taken with a hand-held RGB-D camera, [3] presents a novel method for estimating the spatially varying isotropic surface reflectance under unknown environment illumination. We propose a coherent joint optimization formulation that alternates between solving for plausible camera poses, materials, the environment's lighting, and normal to address the aforementioned issues. We take advantage of the numerous spatial and view-dependent variations of materials to improve imprecise camera localization. The object is treated like a model that self-calibrates for localization. A global optimization that takes advantage of the sparsity in the wavelet domain to efficiently solve is used to recover the unknown lighting by utilizing measured colour images and the current estimate of the materials. A photometric consistency constraint is the primary foundation upon which we also correct incorrect normal.

[2] Three important participants are included in the proposed protocol: an authentication server (AS), an access point (AP), and a client (C). We assume that the AP-AS connection is safe and dependable. The registration phase and the authentication phase are the two phases of the protocol. Client C and authentication server AS share credentials over a secure channel during the registration phase. Instead of using an asymmetric algorithm during the authentication phase, we use a symmetric encryption algorithm and a hash function to meet all security requirements and reduce exponential computation and communication overhead.

By taking advantage of IEEE 802.11 frames at the link-layer level, the proposed attack can inject malware into the application layer. More specifically, the proposed attack encapsulates a spoofed payload that can initiate an airborne malware download and replaces an IEEE 802.11 wireless frame sent by a TCP client node. Through the use of fake ACK spoofing, it deceives the transmitter on the TCP client into believing that the data frame transmission was successful and forces the TCP client to continue waiting for a TCP response packet from the TCP server. A compromised packet eventually infects the TCP client, even though the client does not intend to receive it. At the MAC layer, the proposed attack makes use of SDR technology to generate and transmit fake ACK frames and jamming frames. We can respond to the victims' frames in real-time without the CSMA/CA backoff mechanism thanks to the SDR's ability to override the usual IEEE 802.11 physical/MAC layer operations, in contrast to off-the-self nodes that use the IEEE 802.11 DCF protocol. At the physical layer level, it directly generates and transmits an IEEE 802.11 radio-frequency waveform over the wireless channel.

Table 1 Literature Work Summary

Author	Journal	Work	Outcome
Woocheol Kim	IEEE Access-2021	propose a malicious frame injection-based attack without capturing an AP-client node association. In the shared wireless medium, the proposed attack performs wireless jamming, MAC frame sniffing, and spoofing simultaneously. To demonstrate the threat to wireless LAN security, we	3.45 Time delay and 69 Avalanche for a 128-bit

		used a real-world experimental testbed with pre-existing nodes and software-defined radio (SDR) to carry out the proposed attack and the transmission control protocol (TCP) transport protocol on HTTP communication.	input
Awaneesh Kumar Yadav	IEEE Proceedings 2021	propose an EAP-based authentication protocol for IEEE 802.11 WLANs that is user-friendly and secure. BAN logic and the AVISPA tool have formally validated the proposed protocol [18]. The simulation results show that the proposed protocol meets all RFC-4017 security requirements, including perfect forward secrecy, protection against denial-of-service (DoS) attacks, and light computation.	4.21-time delay
Hongzhi Wu	IEEE Transactions 2016	present an innovative method for estimating the spatially varying isotropic surface reflectance solely from colour and depth images taken with an RGB-D camera in an unidentified lighting environment. Our method is based on a joint optimization that alternates solving for plausible camera poses, materials, lighting in the environment, and normal.	4.35-time delay

3. PROBLEM FORMULATION

Key Size and Management Key management is one of the WEP standard's flaws because it is not specified. This is because keys with poor quality and long lifespans are more likely to be produced without interoperable key management. The majority of wireless networks that use WEP share a single WEP key among all network nodes. Client stations and Access Points (APs) must be programmed with the same WEP key. Keys are rarely changed because it is time-consuming and difficult to synchronize their movement. The issue with the proposed Kerberos extensible authentication protocol (KEAP) is that while it provides adequate protection against MAC Address Spoofing, WEP attacks, and poor network design, KEAP becomes less secure when logical attacks such as Denial of Service attacks and Man-in-the-Middle attacks attempt to penetrate the WLAN network. Additionally, their method is less secure in the event of any kind of physical attack. TKIP performs poorly in the event of a logical attack and does not protect against a Denial of Service attack. It is best suited for physical attack protection. The problem with [2] work was that it only used WEP, which is not secure because of a bad network design. Although WEP is faster than KEAP, it is much less secure than KEAP. After looking at the issues with the existing work, a proposed solution is created that is quick enough and offers good protection against physical and logical attacks. The work that is being proposed makes use of both TKIP and Kerberos.

4. WLAN SECURITY TECHNOLOGIES

Since the early days of the IEEE802.11 standard [1], WEP has been the standard for security. It is used to provide secured authentication schemes and to protect communications between APs and STAs; The objective was to provide the WLAN with security comparable to that of a wired LAN. The "RC4" stream cypher encryption algorithm serves as its foundation. Encryption of sensitive data and access control to the WLAN are both made possible by WEP. Both theoretically and practically, it was established that several issues contributed to WEP's failure as a security protocol. The specifics of WEP and the issues it faces are discussed in references like [3], [4], [12], [4], and [7].

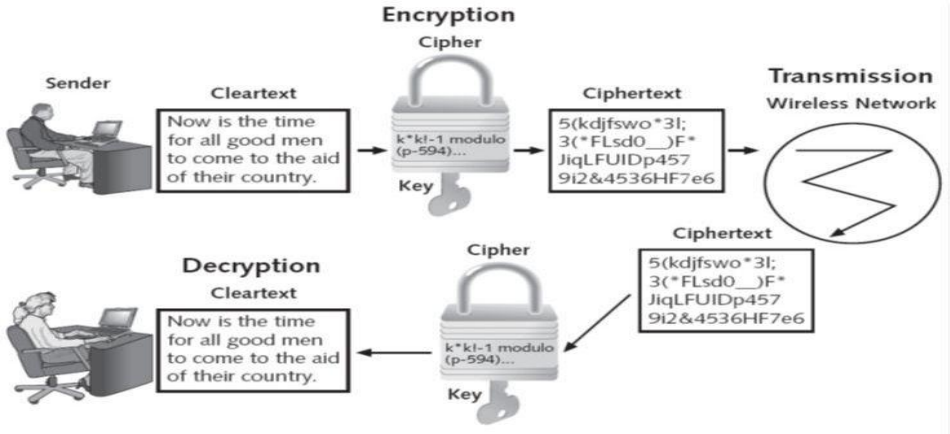

Fig. 2 Schematics of the Wired Equivalent Privacy (WEP) protocol used to control access to the WLAN and to encrypt confidential information.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 02, February 2023, pp : 106-110

e-ISSN : 2583-1062

Impact Factor : 5.725

As shown in equation 1 and Figure 3, a straightforward XOR operation between the WEP encryption key (K) and the plain text message (M) generates the cypher text (C). The encryption key can be obtained by XORing the plain text message with the cypher text, as shown in equation (2). As can be seen, XORing two plain text messages are equivalent to XORing two ciphertext messages.

Decrypts the transmitted data with ease by locating the appropriate WEP key. WEP also lacks solutions for managing keys, has no solid policy for distributing keys, and frequently reuses a single key. This issue will make not only the AP vulnerable to attacks but also all of the other APs and STAs. Even worse, key distribution is static by default, necessitating the manual entry of the key by each STA and the use of a new key if the key is compromised. WEP generally lacks a key distribution and management system. By distributing the keys through a Dynamic Host Configuration Protocol (DHCP) server, Reference [37] suggests a potential solution to the issue of key distribution. WEP keys are distributed by the DHCP server as part of the DHCP frame options. There is no defence mechanism for WEP against replay attacks. An attacker can illegally record a WEP encrypted message and use it multiple times to gain access to the WLAN as a legitimate user or obtain information about the encryption key. WEP is not recommended if high security is required, as it has been mathematically and practically demonstrated to be insecure. However, WEP-protected WLANs provide an additional barrier for attackers and are unquestionably superior to unprotected WLANs.

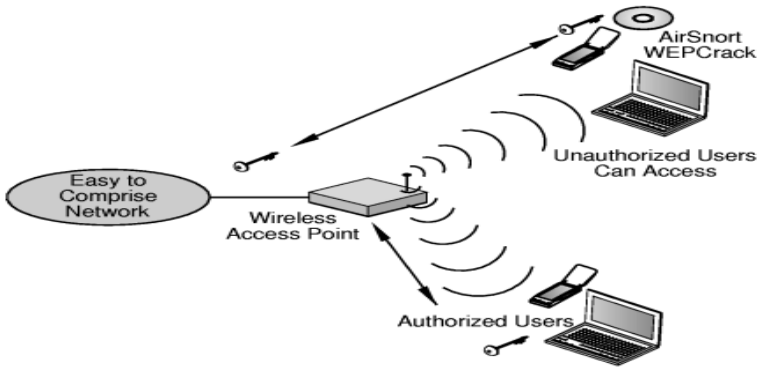

Fig. 3 Illustration of a Wired Equivalent Privacy (WEP) weakness. The attacker can monitor encrypted transmissions and captures IVs.

5. CONCLUSION

IEEE802.11 was initially designed to interconnect wireless devices to wired networks; the aim was to achieve networking with minimum or no security. Security was not an important issue at that stage, however, with the success of WLANs and the fast adoption of this technology, security became important and achieving security became a primary concern. Wired Equivalent Privacy (WEP) security protocols were the first to be adopted in an attempt to satisfy the need for securing wireless networks, soon WEP became vulnerable and there was a demand for a better security protocol. Industries already invested in wireless devices so any new protocol should consider the hardware capabilities of such devices. TKIP came into the picture with the promise of better security using the same hardware.

6. REFERENCES

[1] "Malicious Data Frame Injection Attack Without Seizing Association in IEEE 802.11 Wireless LANs," by W. Kim, S. Kim, and H. Lim, in IEEE Access, vol. 9, pp. 16649-16660, 2021, doi: 10.1109/ACCESS.2021.3054130.

[2] "Secure and User Efficient EAP-based Authentication Protocol for IEEE 802.11 Wireless LANs," K. Yadav, M. Misra, M. Liyanage, and G. Varshney, in 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Delhi, India, 2020, pp. 576-584, doi: 10.1109/MASS50613.2020.00076.

[3] "Simultaneous Localization and Appearance Estimation with a Consumer RGB-D Camera," by H. Wu, Z. Wang, and K. Zhou, published in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 8, pp. doi: 2012-2023, August 1, 2016, 10.1109/TVCG.2015.2498617.

[4] The Improvement of Wireless LAN Security Authentication Mechanism Based on Kerberos, Yi Ma and Hongyun Ning, 2018 International Conference on Electronics Technology, 978-1-5386-5752-2/18/IEEE

[5] Abhijit Bodhe Mayur Masuti Dr A.S. Umesh, Wireless LAN Security Attacks and CCM Protocol with Some Best Practices in Deploying Services, International Research Journal of Engineering and Technology (IRJET) e- 2395-0056 Quantity: 03 Issue: January 2016

[6] Matthew S. Gast, 802.11 Wireless Networks, O'Reilly, 2002

[7] Cryptography and Network Security, Principles and Practices, Third Edition, Prentice Hall, 2003, by William Stallings.

[8] "Implementing Improved WLAN security," by Matija Sorman, Tomislav Kovac, and Damir Maurovic, presented at the 46th International Symposium on Electronics in Marine. Zadar, 2004 ELMAR Croatia, June 16-18, 2004

[9] Derrick Dicoi and Joon S. Park, "WLAN Security: "Now and in the Future." Oct. 2003, IEEE Computer Society

[10] Gary McGraw and Nancy R. Mead. The Future of Wireless Security." IEEE Security and Privacy, August 2003, IEEE Computer Society.

[11] "Providing for Wireless LAN Security, Part 2" by Joseph Williams. November and December 2002 issues of IEEE IT Pro.

[12] Shin, M.; Ma, J.; A. Mishra; W.A. Arbaugh, "Wireless network security and interworking," IEEE Proceedings, Volume 94, Issue 2, February 2006, pages 455–466,

[13] "Wireless LAN and its security problem," by Wang Shunman, TaoRan, WmgYue, and ZhangJi. The Fourth International Conference on Parallel and Distributed Computing, Applications, and Technologies, 2003, was published in its proceedings. PDCAT'2003.