International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0047
ISSN (Online): 2279-0055

International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Review of Existing Security Protocols Techniques and their Performance Analysis in WLAN

Latha.P H
Research Scholar
Visveswaraya Technological University
Belguam, INDIA
Dr. Vasantha R
Prof.: Dept of Information Science Engineering
Sambhram Institute of Technology
Bangalore, INDIA

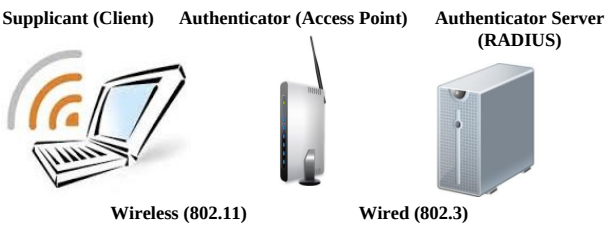
Abstract: *The area of wireless networking is always shrouded by security loopholes where security in Wireless Local Area Network (WLAN) is still yet to be witnessed some full-fledge security incorporation. Majority of the corporate and institutional establishment uses WLAN as it is highly cost-effective and convenient to use. However, various sophisticated attacks like jamming attack, flooding attack, WPA-PSK Attack etc are still on the rise. With the availability of expensive network and security devices, such attacks are yet hard to be mitigated. The past decade has witnessed various formulations of security protocols which claims to address the breaches in IEEE 802.11 standards. This paper presents some of the effective security protocols right from evolution to existing scenario and discusses various pros-and-cons of security protocols in WLAN with respect to its countermeasure techniques on various attacks. The overall outcome of this review paper is that frequently used security protocols are not as robust and sufficient enough to mitigate the possible lethal threats in wireless LAN.*

Keywords: *Attacks in WLAN; Security PSK; Wireless Local Area Network; WPA; WEP.*

I. Introduction

A wireless LAN (or WLAN) is a type of wireless connection where a mobile user can connect to a local area network (LAN) through a wireless (radio) connection [1]. Formulation of such networking system is governed by IEEE 802.11 standards that discusses about the usage as well as security mechanism to be performed over the vulnerable wireless medium. There are two critical parameters of securing WLAN e.g. authentication and encryption [2]. A wireless system mechanizes authentication to evaluate user's credentials and resolve if the user is supposed to be permitted for an access to the data and resources furnished by the protected network. The phenomenon of encryption performs encoding of the data so that anyone who does not have the secret "key" will not be able to read the data. IEEE 802.1x verifies use of port-based access control that means the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" node at each port to thwart illegal users from gaining access to safeguarded data. The 802.1x authentication procedure involves three basic players: i) The supplicant is the client (for example, PC or laptop computer) who would like to gain access to network resources through the wireless network, ii) The authenticator, which for a wireless network is usually an access point (AP), plays the role of gatekeeper, and iii) The authentication server, which connects to the router over a wired network, handles the authentication procedure. Fig.1 signifies the association of supplicant, authenticator, and server. It was also found that majority of the application uses RADIUS server.

Figure 1 Authentication of IEEE 802.1x (WLAN)



In effect, the authenticator and authentication server work as a team to confirm the identity of the supplicant node. The authentication server also takes responsibility for computing the "keys" that the encryption algorithm will use. The sophisticated procedure of encryption is one of the most crucial parameter in WLAN technology. This is because the radio waves used to transmit data packets between user computer and the wireless access point can pass through walls, floors, and other barriers. People who use laptops that have a wireless LAN card will know

this first-hand, since it is often possible to pick up signals from wireless access points located in nearby apartments. Using a password to restrict entry to your network may not provide enough protection, since a reasonably clever person can still intercept your data packets. In fact, if the person intercepting the wireless data is just a tad cleverer than "reasonably clever," he or she may also be able to download and read the contents of the packets. This paper discusses about the various trends of security protocols, their strength and weakness with the support of prior work being carried out in the direction of securing wireless LAN.

II. Security In WLAN

This section will discuss various steps in wireless LAN security with significant review of its current status of implementing 802.11i security protocol. The wireless environment is more challenging to safeguard because of its open broadcast nature [3]. These characteristics create a well secured protocol that is almost equivalent to wired security modules a very challenging job.

A. 802.11 Standard

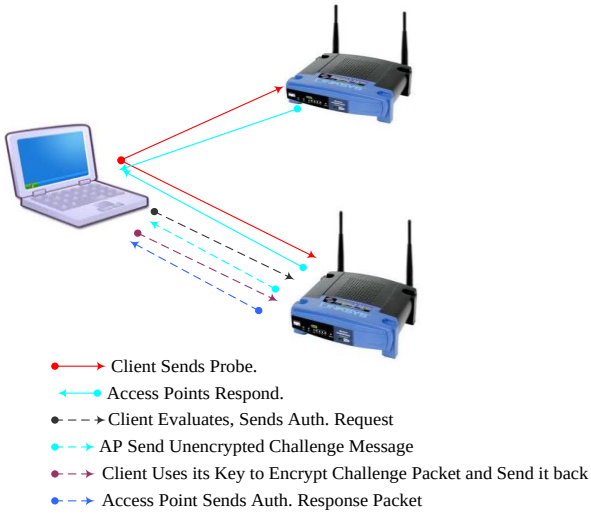
IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands. IEEE 802.11 has three layers: Physical layer, MAC (Medium Access Control) layer, and LLC (Logical Link Control) layer as shown in Fig. 2.

Figure 2 802.11 Layers

LLC		
MAC		
Frequency Hopping	**Direct Sequence**	**Infrared Light**

The designers of IEEE 802.11 standard has considered the requirement of making the physical layer supports more than one signaling technique and interface, as shown in Fig. 2. The physical layer is used for furnishing an interface for exchanging frames using the upper MAC layer, transmitting and signaling packets, and works as a media activity sensor for MAC layer. The MAC layer supports the operation needed to permit the reliable transfer to the upper layers, and it is very equivalent to the data link layer in the Open System Interconnection model (OSI). It furnishes the operations for controlling media access and it is connectionless oriented. The Logical Link Control furnishes addressing and data link control and is free from the lower layers i.e. MAC and PHY. Logical Link Control also furnishes connection oriented service to the upper layers.

Figure 3 Shared Key Authentication



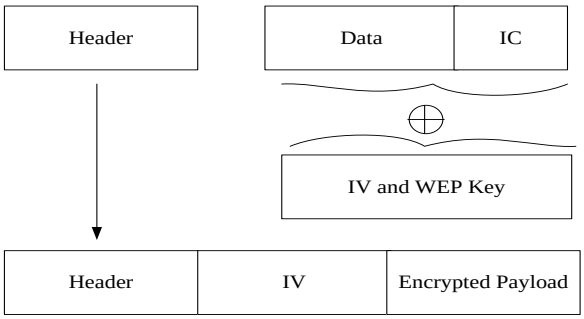
To permit the clients to access the network they must go through two steps: getting verified by the access point in WLAN and then getting connected (authorization). According to Earle [4], there are two types of authentications e.g. Shared Key Authentication and Open Key Authentication. Similar Scheme was seen to be used by Sithirasenan [5]. In the Wired Equivalent Privacy standard, which is the first security module used with 802.11, both of the authentication modes were supported. However, in the new security standards, it is not suggested to use shared key authentication. Fig. 3 below shows how Shared Key Authentication works.
The client sends a request when it wants to connect to the WLAN router. Upon that request, the WLAN router sends a challenge packet in clear text which is not encrypted. The client then encrypts it using its WEP key and

transmits back. The WLAN router then attempts to decipher the encrypted message using its WEP key. If the decryption process is successful then it means that the client is a legitimate user or else the access is denied for that specific user. Moreover, if any illegitimate member in the network is attempting to sniff the data packet then they will get a copy of the encrypted data. With some time and processing power the WEP key can be found. Open Key Authentication does not involve challenge/response messages exchange. The client will always get authenticated, but to transmit and receive messages, the client needs to have the precise WEP key. Although Open Key Authentication does not offer any kind of verification process, it is more secure. The motive behind this is that Open Key Authentication does not expose the WEP key to traffic sniffers.

B. Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an easily broken security algorithm for IEEE 802.11 wireless networks to provide data confidentiality comparable to that of a traditional wired network. WEP has three goals to achieve for wireless LAN: confidentiality, availability and integrity [4]. WEP uses encryption to provide confidentiality between the client and the AP, meaning that packet transfers after the AP (wired LAN) are unencrypted. WEP uses RC4 for the encryption purposes. Since RC4 is a stream cipher it needs a seed value to start its key stream generator. This seed is called IV (Initialization Vector). The IV and the shared WEP key are used to encrypt/decrypt transferred packets (Fig. 4). In the encryption process, the Integrity check (IC) value is computed and attached to the payload, then the payload is XORed with the encryption key consisting of two sections (IV and WEP Key). The packet is then forwarded with the IV value sent in plain text as shown in Fig.4

Figure 4 WEP Packet Encryption



WEP uses CRC (Cyclical Redundancy Checking) to verify message integrity. On the other side (receiver: AP) the decryption process is the same but reversed. The AP uses the IV value sent in plain text to decrypt the message by joining it with the shared WEP key.

B.1 Weaknesses of WEP

One of the major reasons behind WEP weaknesses is its key length. WEP has a 40-bit key, which can be broken in less than five hours using parallel attacks with the help of normal computer machines [6]. This issue urged vendors to update WEP from using 40-bit to 104-bit key; the new release is called WEP2. This update helped to resolve some security issues with WEP. The main disadvantage of WEP however, is the lack of key management. In addition to that, WEP does not support mutual authentication. It only authenticates the client, making it open to rouge AP attacks. Another issue is the use of CRC to ensure integrity. While CRC is a good integrity provision standard, it lacks the cryptography feature. CRC is known to be linear. By using a form of induction, knowing enough data (encrypted packets) and acquiring specific plaintext, the WEP key can be resolved [6] . RC4 suffers from a deadly symptom. It tends to repeat IV values (even if it is auto generated), making the exposing of the traffic easier. Mathematically, if the same IV is used to encrypt two packets (WEP key did not change also) and if somebody has a pair of encrypted/plaintext message, then by applying the following simple rule:

$$C1 \text{ XOR } C2 = P1 \text{ XOR } P2$$

it is very easy to know the content of the new encrypted packet P2 , if P1,C1 and C2 are already known [7]. These weaknesses forced the designers of WLAN security modules to be more cautious. It demonstrates the result of not designing the security module from the ground up taking into consideration all applicable risks. In the next section we will go through the new standards that came after WEP to overcome its vulnerabilities.

B.2 Attacks on WEP

The prior studies have discovered security problems that let malicious users compromise the security of WLANs that use WEP. The various attacks in WEP witnessed in past studies are as follows:

- ***Chopchop Attack:*** This attack was proposed with the pseudonym KoreK in 2004 [8]. The attacker can decrypt the last s bytes of plaintext of encrypted packet by sending an average of s*128 packets

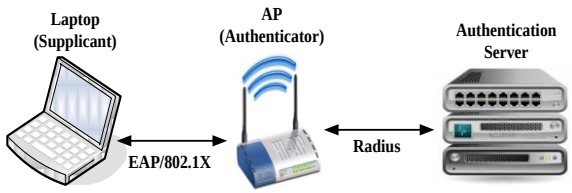
on the network. Integrity Check Value (ICV) is appended with the plain text and chopchop attack exploits the insecurity of this four byte checksum. The root key is not revealed in this attack. Various access points can easily identify between correct and incorrect checksum of encrypted packets. The attacker chops one byte from end of captured packet, guesses the packet's last byte and modifies the checksum accordingly and sends the packet to access point. If the guess was correct, the access point accepts the packet and the attacker now knows the last byte of plaintext. So, attacker proceeds to determine the second last byte.

- ***Bittau's fragmentation Attack**:* In this type of attack, after attacker discovers keystream of length s, he can send packets with payload length s-4 i.e. excluding 4 byte ICV. Long packets can be split up to 16 fragments with s-4 payload length per packet. These fragments are received and reassembled as a single packet at the access point. The packet is re-encrypted with a new key stream and transmitted by the access point. Since the attacker knows the plain text, attacker can easily recover new key stream. [9]
- ***Fluhrer, Mantin and Shamir (FMS) Attack**:* The most serious attack on WEP was discovered by three cryptographers: Fluhrer, Mantin and Shamir. FMS attacks are due to use of weak initialization vectors in RC4 algorithm [10] [11]. The encrypted packets along with initialization vectors for these packets can be recorded by listening passively to network traffic. The attacker is easily able to recover the first bytes of keystream which were used for packet encryption, since first bytes of plaintext can be easily predicted. The attacker can also easily know the initialization vector (first three bytes of per packet key) which is transmitted unencrypted with the packets. Rests of the bytes per packet key are unknown to attacker but are identical for all packets. Thus, the attacker gathers a large amount of encrypted data and generates different possible values. The actual value appears more frequently than any other value enabling the attacker to recognize the correct key value. Various tools like WEP Crack, AirSnort and bsd-airtools [12] have automated WEP cracking.
- ***Pyshkin, Tews and Weimann (PTW) Attack**:* This attack was introduced in 2007 and utilizes the analysis of RC4 stream cipher showing further associations between RC4 key streams and key presented by Andreas Klien in 2005 [13]. The probability of this attack being successful is independent of key byte being attacked unlike FMS and KoreK attack. Also, it utilizes more number of bytes of key stream and byte count which depends upon length of IV and secret root key. PTW attack requires 85,000 frames with 95% probability of successful execution i.e. breaking 104 bit WEP key unlike FMS attack which requires 10 million messages [14].

C. 802.1x

The 802.1x standard was designed for port base authentication for 802 networks. 802.1x does not care what encryption techniques is used, it is only used to authenticate users. IEEE 802.1x defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as "EAP over LAN" or EAPOL [15][16].

Figure 6 802.1x Authentication



The 802.1x framework defines three ports or entities: Supplicant (client want to be authenticated), Authenticator (AP that connect the supplicant to the wired network), and Authentication Server (abbreviated AS which performs the authentication process from the supplicant based on their credentials) [17]. The authentication server in the 802.1x framework uses RADIUS (Remote Authentication Dial-In User Service) protocol to provide AAA (Authentication, Authorization and Accounting) service for network clients [18]. The protocol creates an encrypted tunnel between the AS (Authentication Server) and the Authenticator (AP). Authentication messages are exchanged inside the tunnel to determine if the client has access to the network or not. Fig.6 shows the network layout.

D. 802.11i Standard

IEEE 802.11i implemented as WPA2, is an amendment to the original IEEE 802.11. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. After the final release of 802.11i the vendors implemented the full specifications under the name WPA2 [19]. 802.11i supports two

methods of authentication. The first method is the one described before by using 802.1x and EAP to authenticate users. For users who cannot or do not want to implement the first method, another method was proposed to use per-session key per-device. This method is implemented by having a shared key (like the one in WEP) called GMK (Group Master Key), which represent the base key to derive the other .GMK is used to derive PTK (Pair Transient Key) and PSK (Pair Session Key) to do the authentication and data encryption. To solve the integrity problem with WEP, a new algorithm named Michael is used to calculate an 8-byte integrity check called MIC (Message Integrity Code). Michael differs from the old CRC method by protecting both data and the header. Michael implements a frame counter which helps to protect against replay attacks [20] .

To improve data transfer, 802.11i specifies three protocols: TKIP, CCMP and WRAP. TKIP (Temporal Key Integrity Management) was introduced as a "band-aid" solution to WEP problems. One of the major advantages of implementing TKIP is that you do not need to update the hardware of the devices to run it. Simple firmware/software upgrade is enough. Unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism [21] . TKIP ensures that every data packet is sent with its own unique encryption key. TKIP is included in 802.11i mainly for backward compatibility. WRAP (Wireless Robust Authenticated Protocol) is the LAN implementation of the AES encryption standard introduced earlier. It was ported to wireless to get the benefits of AES encryption. WRAP has intellectual property issues, where three parties have filed for its patent. This problem caused IEEE to replace it with CCMP.

CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) is considered the optimal solution for secure data transfer under 802.11i. CCMP uses AES for encryption. The use of AES will require a hardware upgrade to support the new encryption algorithm.

E. Robust Secure/Security Network

RSN (Robust Secure/Security Network) is a part of 802.11i for providing a method to exchange the clients and the AP capabilities of implementing security methods. RSN uses RSN IE (Information Element) frames to exchange this type of information. RSN increases the flexibility of wireless security network standards and provides options to define the security policies implemented in organizations [22].

III. WI-FI Protected Access

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks [23]. WPA was intended to address the WEP cryptographic problems without requiring new hardware.

A. WPA Encryption Process:

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption [24]. A new key is dynamically generated for every packet; 128 bit per packet key is used. Michael algorithm is used by TKIP to generate Message Integrity Code (MIC) which provides enhanced data integrity as compared to CRC-32 used in WEP. Also, TKIP provides replay protection.

B. WPA Authentication Mechanisms:

The two authentication mechanisms provided by WPA are:

- WPA-Personal or WPA-PSK (Pre-Shared Key): Pre-Shared Key is a static key shared between two parties for initiating the communication. The key which is a Pairwise Master Key (PMK) in TKIP process must be in place before an association can be established [25]. WPA-Personal is suitable for home and small office networks and an authentication server is not required. The wireless devices are authenticated with access point using 256 bit key. The key is never transmitted over air since station and access point already possess this key before initiating the communication. Also, 64 bit MIC key and 128 bit encryption key can be derived from pre shared key.
- WPA-Enterprise: This is designed for enterprise networks. IEEE 802.1x and Extensible Authentication Protocol (EAP) provide stronger authentication. In this mode, Remote Authentication Dial In User Service (RADIUS) server is required which provides excellent security for wireless network traffic. The various EAP methods are EAP- Lightweight Extensible Authentication Protocol (EAP- LEAP), EAP- Flexible Authentication via Secure Tunneled (EAP-FAST), EAP- Message Digest 5 (EAP-MD5), EAP- Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), EAP- Subscriber Identity Module of Global System for Mobile Communications (EAP-SIM) [26].

C. WPA Shortcomings

- WPA uses old cryptography algorithm RC4 instead of superior Advanced Encryption Standard (AES).
- WPA is vulnerable to brute force attacks in case of weak passphrase for pre shared key mode.
- Prone to threats during Hash collisions due to use of hash functions for TKIP key mixing.
- WPA remains vulnerable to availability attacks like Denial of Service.
- WPA has greater performance overhead unlike WEP.
- Complicated setup is required for WPA-enterprise.

D. WPA2 Shortcomings

- Prone to availability attacks like Jamming and Flooding since it cannot prevent physical layer attacks [27].
- Control Frames like Request to Send (RTS) and Clear to Send (CTS) are unencrypted making them prone to DoS attacks.
- Management frames that are used to report network topology are not encrypted thus enabling attacker to analyse the network layout.
- GTK is shared amongst all authorized clients of the network. A malicious authorized client may inject spoofed GTK packets in the network. Thus, an authorized user can sniff and decrypt data of other authorized users and may install malware and compromise other user's devices [28]. This is known as Hole196 vulnerability. WPA/WPA2 Enterprise which is based on port-based 802.1X access control protocol is prone to this vulnerability.
- WPA 2 is expensive for the already deployed networks since CCMP and AES implementation needs change in the existing network hardware.
- De-authentication may lead to MAC address spoofing.

E. Attacks on WPA

TKIP used in WPA is prone to Chopchop, Ohigashi-Morii, WPA-PSK and Beck-Tews attack [29]. WPA-PSK Attack: Authentication mechanisms WPA-PSK is prone to offline dictionary attack since information has to be broadcasted for verification of session key. In order to generate PMK, passphrase, Service Set Identifier (SSID) and SSID length are fed into hashing algorithm. Since SSID can be easily recovered thus, in order to identify PMK only passphrase needs to be guessed. There is approximately 2.5 bits of security per character in passphrase. Thus, n bytes passphrase leads to key with 2.5n+12 bits of security strength and hence, vulnerable to dictionary attack in case of short passphrase i.e. less than 20 characters. Hence, if PMK is determined by attacker, he can gain access to the network. Aircrack and coWPAtty [28] are the tools which can be used for attack.

- ***Beck-Tews Attack****:* This attack is an extension to chopchop attack on WEP. Since, TKIP implements MIC, so if two MIC failures are observed within 60 seconds then both client and access point are shut down and TKIP session key is rekeyed. Thus, in case of failure, the attacker waits for 60 seconds to avoid countermeasures. Packet can be decoded at rate of one byte per minute with this attack. Once plaintext has been retrieved by attacker, he has access to MIC and keystream of packet which he can use to construct and transmit a new packet on network and in turn enabling the attacker to execute Denial of service and ARP poisoning attacks [29][30]. This attack can be executed only against TKIP and not against WPA implementing AES.
- ***Ohigashi-Morii Attack****:* This attack [31] uses a mechanism similar to Beck-Tews attack but also executes a man in the middle attack. Unlike Beck-Tews, it is efficient for all WPA modes and does not require Quality of Service to be enabled on access point.
- ***Michael Reset Attack****:* This attack was discovered by Beck and Tews [32] and was based on flaws in Michael. During the initialization phase of Michael, two keywords are set as the internal state which processes following 32 bit words. Also, the Michael algorithm resets when internal state reaches a particular point which results in rest of plaintext to have same MIC as of the whole packet. Thus, it enables the attacker to add any plaintext along with keyword to reset the algorithm which

results in packet modification without affecting the correctness of Michael's result. This attack involves discovering magic words which are put in between arbitrary captured packet and ICMP echo request. This echo request is transmitted to client on wireless network with spoofed IP address of attacker port which in turn causes ICMP response to be delivered to the attacker port, thus, enabling the attacker to decrypt the captured packet.

Table I Extensive Review of the Security protocols in Wireless LAN.

	WEP	WPA	WPA2
Key length	40 bits or104 bits	128 bits encryption	128 bits or higher
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and keys are generated through four way handshake	Provides robust key management and keys are generated through four way handshake
Hardware Compatibility	Works on existing hardware	Works on existing hardware through firmware upgrades on NIC	Supported in Wi-Fi devices certified since 2006, Does not work with older NIC
Attacks/ Vulnerabilities	Chopchop, Bittau's fragmentation, FMS and PTW attack, DoS attacks	Chopchop, Ohigashi-Morii, WPA-PSK, Beck-Tews and Michael Reset Attack and Hole 196 vulnerability, DoS attacks	Hole 196 vulnerability, DoS attacks due to unencrypted management and control frames, MAC address spoofing due to De-authentication, Offline dictionary attacks in WPA2-Personal
Deployment complexity	Easy to setup and configure	Complicated setup required for WPA-enterprise	Complicated setup required for WPA2-enterprise
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	48 bit packet number prevents replay attacks

IV. Security Tools

The existing security tools for ensuring security in wireless LAN are as follows:

- ***AirDefense™:*** It is a commercial wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks, and assists in the management of a WLAN. AirDefense also has the capability to discover vulnerabilities and threats in a WLAN such as rogue APs and ad hoc networks. Apart from securing a WLAN from all the threats, it also provides a robust WLAN management functionality that allows users to understand their network, monitor network performance and enforce network policies [33].

- ***Isomair Wireless Sentry:*** This product from Isomair Ltd. [34] automatically monitors the air space of the enterprise continuously using unique and sophisticated analysis technology to identify insecure access points, security threats and wireless network problems. This is a dedicated appliance employing an Intelligent Conveyor Engine (ICE) to passively monitor wireless networks for threats and inform the security managers when these occur. It is a completely automated system, centrally managed, and will integrate seamlessly with existing security infrastructure. No additional man-time is required to operate the system.

- ***Wireless Security Auditor (WSA):*** It is an IBM research prototype of an 802.11 wireless LAN security auditor, running on Linux on an iPAQ PDA (Personal Digital Assistant) [35]. WSA helps network administrators to close any vulnerabilities by automatically audits a wireless network for proper security configuration. While there are other 802.11 network analyzers such as Ethereal, Sniffer and Wlandump, WSA aims at protocol experts who want to capture wireless packets for detailed analysis. Moreover, it is intended for the more general audience of network installers and administrators, who want a way to easily and quickly verify the security configuration of their networks, without having to understand any of the details of the 802.11 protocols.

V. Prior Studies

The past decade has witnessed thousands of the solutions being offered in the literature that claims to be potential enough for providing security over WLAN. Each of the literature has their own architectures and policies; some are evaluated in real-time while some in simulated study. It was also seen that none of the literature has yet proved fruitful in mitigating the security breaches in Wireless Environment till date. 802.11i standard for wireless local networks introduces WEP protocol to try to solve the problems of protection and to make the level of protection of wireless local networks similar to the protection level of wired local networks. However, some of

the potential studies carried out in past to address the security issues of protocols in WLAN are briefly discussed here.

Mavridis et al. [36] have presented a brief overview of them, focusing on three main security protocols WEP, WPA and WPA2. The authors have discussed and presented in detail an analytical procedure towards WEP and WPA2 cracking, derived from real-life situations. Their motivation was the need for increased wireless security and the common feel that nowadays WPA/WPA2 security protocols are difficult for a stranger to hack; however, their study depicted that any wireless network may be suffering from successful hacking attempts, if it is not carefully setup and protected.

Haddadi et al [37] have proposed a hybrid wireless intrusion detection system (WIDS). To implement the WIDS, they designed a simple lightweight agent. The proposed agent detects the most destroying and serious attacks; Man-In-The-Middle and Denial-of-Service; with the minimum selected feature set. To evaluate their proposed WIDS and its agent, they collect complete data-set using open source attack generator software. Experimental results show that in comparison with similar systems, in addition of more simplicity, their WIDS provides high performance and precision.

Odhiambo et al. [38] have demonstrated an integrated security model (ISM) that incorporates a drop policy to defend against DoS attacks. They assume the use CCMP to provide Confidentiality and Integrity and use EAPTILS/ 802.11 xs with RADIUS to provide authentication. They use simulation in OPNET to show that their security model performs better to provide improved security in terms of confidentiality, integrity, authenticity and availability.

Bittau et al. [39] have presented a novel vulnerability which allows an attacker to send arbitrary data on a WEP network after having eaves dropped a single data packet. Furthermore, they present techniques for real-time decryption of data packets, which may be used under common circumstances.

Liu et al. [40] have illustrated an overview of WPA/WPA2 is supplied. And then, the vulnerabilities of WPA/WPA2 and current researches in the method of attacking WPA/WPA2 are introduced. In the last part, these researches are analyzed and concluded.

Sherman et al. [41] have developed for the UMBC Cyber Defense Lab cover a variety of important and timely IA topics. The vulnerability scanning exercise, the first of their exercises to be used in the classroom, received overwhelmingly positive reactions from students, who appreciated the practical, hands-on learning activities related to a useful and interesting topic.

Jagetia and Kocak [42] have proposed a scrambling algorithm that reduces the vulnerability of the WEP. Both the software and hardware implementations of the algorithm reveal at least 10,000 times improvement in security.

Tsukaune et al. [43] presented a secure WEP operation against key recovery attacks. The proposed method requires for attackers at least 100,000 packets to recover the WEP key. Furthermore they theoretically evaluate their technique to operate a secure WEP communication.

Nobles and Horrocks [44] have focused upon flaws in the WEP encryption and authentication processes. There exist, however, vulnerabilities in the lower layers of the protocol stack that may be easily exploited to produce denial of service attacks. One area to exploit is the medium access control (MAC) protocol that aims to ensure availability and fair sharing of the available wireless bandwidth.

Omar et al. [45] have illustrated their work targets networks secured by the Wired Equivalent Privacy (WEP) protocol because of its widespread use and vulnerability to a multitude of security threats. By exploiting the existing ARQ protocol in the 802.11 standard, their proposed opportunistic secrecy scheme is shown to defend against all known passive WEP attacks.

From the literature, it can be visualized that WEP is the first protocol for data protection in wireless networks whose mechanism is designed to achieve three safety goals: authentication, confidentiality and message integrity. This mechanism is based on RC4 algorithm (an algorithm that can be trusted) but, still, WEP does not achieve safety goals completely. Basic WEP deficiencies come from unsafe authentication, repeated use and open transfer of IV, key management system and a mechanism for the protection of message integrity that is not applied properly. Although WEP protocol uses RC4 algorithm that is highly reliable, there are several safety deficiencies. All these deficiencies can lead to many threats to WEP safety goals.

VI. Conclusion

This review paper presents various techniques explored in the past for securing Wireless LAN. The overall research conclusion done in this paper is that frequently used security protocol named as 'WEP' is found to be unable to furnish security against various threats and attacks. It is also seen that WPA was introduced as an interim solution to the security flaws identified in WEP. However, from the evidences put forward in the past research works, it can be only said that such wireless security standards are still prone to various attacks like Beck-Tews, Chopchop etc. The recent version of WPA2 is considered as an enhancement over WPA. WPA2 provides some potential encryption procedure by using block cipher AES but it is still vulnerable to attacks due to sharing of GTK among clients and transmission of unencrypted control and management frames. Moreover, WPA2 does not support legacy hardware unlike WPA. Hence, by observing the recent trend in the maximization of user base in wireless environment, there is a need to provide a solution to WPA2 deficiencies in order to secure wireless networks against such lethal attacks.

VII. References

[1] B.W. Putman, "802.11 WLAN Hands-on Analysis: Unleashing the Network Monitor for Troubleshooting &optimization", Author House Computers, pp.292, 2005

[2] M.Mallick, "Mobile & Wireless Design Essentials", John Wiley & Sons, 2003

[3] W.A.Arbaugh,"Wireless security is different". Computer, Vol. 36, Issue.8, pp. 99-101, 2003

[4] A.E.Earle, "Wireless Security Handbook," Auerbach Publications, pp.348, 2005

[5] E.Sithirasenan, V. Muthukkumarasamy, D.Powell, "IEEE 802.11i WLAN Security Protocol – A Software Engineer's Model", AusCERT, pp.122-126, 2005

[6] B.Brown, "802.11: the security differences between b and I", IEEE Potentials, Vol.22, Issue.4, pp. 23-27, 2003

[7] D.Welch., S. Lathrop., "Wireless security threat taxonomy," Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society , pp.76-83, 2003

[8] E.Tews, "Attacks on the WEP protocol", Cryptology ePrint Archive, pp.471, 2007

[9] A. Bittau, "The Fragmentation Attack in Practice", pp.1-13, 2005

[10] M.Beck, E.Tews, "Practical attacks against WEP and WPA", WiSec '09: Proceedings of the second ACM conference on Wireless network security, New York, USA, pp.79-86, ACM, 2009

[11] Andrea Bittau, Mark Handley, Joshua Lackey. The final nail in WEP's coffin, IEEE Symposium on Security and Privacy IEEE Computer Society, pp.386-400, 2006

[12] Bragg, "Network Security: The Complete Reference", Tata McGraw-Hill Education, pp. 815, 2004

[13] A. Klein, "Attacks on the RC4 stream cipher, Designs", Codes and Cryptography, Vol.48, pp.269-286, 2008

[14] E.Tews, R-P.Weinmann,A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", Proceedings of the 8th international conference on Information security applications, Springer-Verlag Berlin, Heidelberg, pp. 188-202,2007

[15] B.Aboba, "Extensible Authentication Protocol (EAP)",http://www.ietf.org/rfc/rfc3748.txt, pp.1-67,2004

[16] "EEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication Key Management", retrieved from www.javvin.com/protocol8021X.html

[17] T.Hardjono,L.R.Dodeti, "Security In Wireless LANS And MANS ," Artech House Publishers, pp.243, 2005

[18] RADIUS - Wikipedia, the free encyclopedia", retrieved from http://en.wikipedia.org/wiki/RADIUS Wikipedia definition and related resources about RADIUS

[19] "Wi-Fi Protected Access - Wikipedia,", retrieved from http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, Wikipedia definition and related resources about WPA

[20] "Overview of the WPA wireless security update in Windows XP" retrieved from http://support.microsoft.com/?kbid=815485 Explains the security features in WPA

[21] "TKIP - Wikipedia", retrieved from http://en.wikipedia.org/wiki/TKIP , Wikipedia definition and related resources about TKIP

[22] http://www.aricent.com/software/80211irobust-security-network-association-rsna.html

[23] "National Institute of Standards and Technology NIST 800-97", retrieved from Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[24] B.Mitchell, "WPA - Wi-Fi Protected Access An Article from Computing", Wireless/networking. Retreived from http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm, 2004

[25] A.Mishra, W.A. Arbaugh, "An Initial Security Analysis of The IEEE 802.1X Standard", University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Technical Report CS-T R-4328 and UMIACS-TR, 2002

[26] http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[27] J. C. M. Changhua, "Security Analysis and Improvements for IEEE 802.11i", 12th Annual Network and Distributed System Security Symposium, pp.90-110, 2005

[28] S.Bosworth, M. E. Kabay, E.Whyne, "Computer Security Handbook", John Wiley & Sons, Computers – pp.1856, 2012

[29] V. Moen, H. Raddum, K. J. Hole, "Weakness in the Temporal Key Hash of WPA", ACM SIGMOBILE Mobile Computing and Communications Review, pp.76-83, 2004.

[30] D.Mark, Ciampa, "Security Guide to Network Security Fundamentals", Cengage Learning- Computers , pp.608, 2011

[31] T. Ohigashi, M. Morii, "A Practical Message Falsification Attack on WPA", JWIS, 2009

[32] M.Beck, "Enhanced TKIP Michael Attacks", retrieved from http://ulozto.net/xUQzC84/enhanced-tkip-michael-attacks-pdf, 2010

[33] "Motorola Air Defense Services Platform", Product spec sheet, Motorola, 2010

[34] M.Thomas, D.Stoddard, "Network Security First-step", Cisco Press Computers, pp. 423, 2011

[35] http://www.research.ibm.com/gsal/wsa/

[36] I.P.Mavridis, A-I.E.Androulakis, A.B.Halkias, P.Mylonas, "Real-Life Paradigms of Wireless Network Security Attacks," Informatics (PCI), 2011 15th Panhellenic Conference, pp.112-116, 2011

[37] F.Haddadi, M.A.Sarram, "Wireless Intrusion Detection System Using a Lightweight Agent," Computer and Network Technology (ICCNT), 2010 Second International Conference, pp.84-87, 2010

[38] O.N.Odhiambo, E. Biermann, G.Noel, "An integrated security model for WLAN," AFRICON, 2009. AFRICON '09. Pp.1-6, 2009

[39] A.Bittau, M.Handley, J.Lackey, "The final nail in WEP's coffin," Security and Privacy, 2006 IEEE Symposium, pp.15-400, 2006

[40] Y.Liu, Z.Jin, Y.Wang, "Survey on Security Scheme and Attacking Methods of WPA/WPA2," Wireless Communications Networking and Mobile Computing (WiCOM), 6th International Conference, pp.1-4, 2010

[41] A.T.Sherman, B.O.Roberts, W.E.Byrd, M.R.Baker, J.Simmons"Developing and delivering hands-on information assurance exercises: experiences with the cyber defense lab at UMBC," Information Assurance Workshop, Proceedings from the Fifth Annual IEEE SMC , pp.242-249, 2004

[42] M.Jagetia, T.Kocak, "A novel scrambling algorithm for a robust WEP implementation [wired equivalent privacy protocol," Vehicular Technology Conference, IEEE 59th , vol.5, pp.2487-2491, 2004

[43] T.Tsukaune, Y.Todo, M.Morii, "Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation," Information Security (Asia JCIS), Seventh Asia Joint Conference, pp.25-30, 2012

[44] N.Phil, A.P. Horrocks. "Vulnerability of IEEE802. 11 WLANs to MAC layer DoS attacks." pp. 14-14, 2004

[45] Y.Omar, M.Youssef, E.H. Gamal,"ARQ secrecy: From theory to practice," Information Theory Workshop, ITW. IEEE, pp.6-10, 2009

Latha P.H. is currently working as a Assistant Professor at Atria Institute of Technology in Dept of Information Science, Bangalore, since 20011. She has total of 15 years of experience in teaching field. After completion of graduation from B.M.S College of Engineering in Information Technology in 1992, she has completed her Master's of Science in Information Technology from KSOU Mysore in 2005 and Masters of Technology in Computer Network Engineering at A.M.C College of Engineering, Bangalore, in 2008. Currently she is an research scholar at Visveswaraya Technological University, Belguam, India. Her research interest includes security in networks.

Dr. R. Vasantha is presently working as Professor in Sambhram Institute of Technology, Department of Information Science and Technology, Bangalore. After completion of Ph.D from Indian Institute of Science (Bangalore), she has accomplished potential 14 years of experience working as research associate in University of New South Wales (Sydney), University of East Anglia (England), Indian Institute of Science (Bangalore). She has also worked as Assistant professor in University of Oklahoma, Oklahoma (USA) and University of Cleveland (USA). Her research interest includes Applied Mathematics like Fluid Dynamics, Numerical Analysis, Computational techniques, Image processing, Pattern recognition, Algorithms, Graph Theory, and teaching in pure and applied mathematics, Finite Automata and Formal Languages, Cryptography.