Wireless Security Using Wi-Fi Protected Access 2 (WPA2)

Miss.Prastavana[1] , Mrs. Suraiya Praveen[2]
1.student of Jamia Hamdard University ,delhi
2. Assistant Professor in computer science department

Abstract

In the recent year we have huge development of wireless technology. We are presently getting more subjects to wireless technology. As we know wireless networks have broadcast nature so there are different security issues in the wireless communication. The security conventions intended for the wired system cannot be extrapolated to wireless systems. Hackers and intruders can make utilization of the loopholes of the wireless communication. This report defines the different remote security dangers to wireless system and conventions at present accessible like wired equivalent privacy (WEP), Wi-Fi protected access(WPA) and Wi-Fi protected access2 (WPA2) . WPA2 is more security convention as compared to Wi-Fi protected access (WPA) it utilizes the Advanced Encryption standard (AES) encryption. In order to eliminate threats and to improve security of wireless network This paper will first discuss the technologies needs and threats to wireless network and avoid these threats using the Wi-Fi Protected Access 2 (WPA2) protocol used to secure communications in Wireless Networks over previous protocols and then it will discuss the available modes to secure a wireless network using the Wi-Fi Protected Access 2 (WPA2) protocol and finally explore its vulnerabilities.

1. Introduction

Wireless communication is the exchange of data between two or more points that are not joined through electrical connection, the most well known wireless technologies use electromagnetic wireless telecommunication, for example, radio. With radio waves distances could be short, for example a couple of meters for TV remote control or the extent that thousands or even huge number of kilometer for profound space radio communication. It includes different sorts of fixed mobile and portable applications, including two way radios, cell phones individual PDAs and wireless networking.

Figure 1 shows an example of wireless communication. The various available wireless l technologies differ in local availability, coverage range and performance, and in some circumstances, user must be able to employ multiple connection types and switch between them using related technologies.

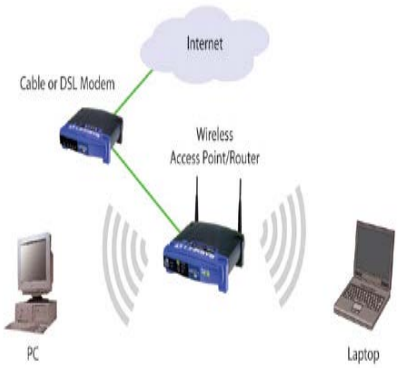


Figure 1 simple wireless communication

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to internet. Standardized as IEEE 802.11 a/b/g/n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become normal standard for access in private homes, within offices, and public hotspots. Wireless Wide Area Network (WWAN) - This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop. These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN. Wireless Personal Area Network (WPAN) - These networks are very similar to WWAN except their range is very limited. Wireless Local Area Network (WLAN) - This network enables you to access the Internet in localized hotspots via a wireless local area network (WLAN) access card and a PDA or laptop. It is a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes. These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is very limited. Wi-Fi is the most widespread and popular example of WLAN technology. Wireless Metropolitan Area Network (WMAN) - This network enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN).These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network.

2. Background Study

This chapter is concern of the wireless security using Wi-Fi Protected Access 2(WPA2).Before discussing Wi-Fi protected access 2, discuss background study has been Related to wireless Security.

2.1Need of Wireless Security

Security is one of important challenge which is to be handled in the era of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. Every time new vulnerability comes in existence to the existing wireless standards. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have pre -installed wireless cards. However, the wireless networking has many security issues but the ability to enter in a network using wireless technology has great benefits over the wired connection. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless intrusion Prevention Systems are commonly used to enforce wireless security policies.The risks to users of wireless technology have increased as the service has become more popular. However there are many securities associated with the current wireless protocol and encryption methods in the carelessness and ignorance that exist at the user and corporate IT level. Cracking method has become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy to use windows or Linux- based tools being made available on the web at no charge.

2.2 Security threats to wireless networks

Protection of wireless networks means protection from attacks on confidentiality, integrity and availability. Possible threats come from vulnerabilities in the security protocols. This section explains various types of security attack techniques. These techniques can be applied to violate both confidentiality and integrity or only confidentiality and only integrity [1].

Traffic Analysis: This technique enables the attacker to have the access to three types of information. The first type of information is related to identification of activities on the network. The second type of information for attacker is important to get the identification and physical locations of access point in its surroundings. This third type of information for an attacker can be obtained by traffic analysis of the information about the communication protocol. An attacker needs to gather the information about the size and the number of the package over a certain period of time.

Eavesdropping: In case of eavesdropping attacker secretly listens to the private conversation of others without their permission. Eavesdropping attacks include passive eavesdropping, active eavesdropping with partially known plaintext and active eavesdropping with known plaintext. Passive eavesdropping is use to watch over an unlimited wireless session. In active eavesdropping with partially known plaintext type attack, the attacker watches over a wireless session an actively injects own message in order to reveal the content of the messages in session.

Man in middle attack enables data reading from the session. There are several ways to implement this type of attacks. One way is when attacker disrupts the session and does not allow for the station to establish communication again with the Access Point; AP station tries to establish session with the wireless network through AP, but can do that only through the work station of the attacker pretending to the AP. At the same time attacker establishes connection an authentication with the AP, now there are two encrypted tunnels instead of one is established between attacker and AP, while the second one is established between attacker and the station. This enables attacker to have the access to the data exchanged between the working station and rest of the network.

ARP attack is a sub type of man in the middle attack since these attacks are directed towards one component of the wireless clients. The attacker escapes authentication or provide false accreditations by this kind of attack.

In high-jacking type of attack, the attacker deprives the real owner of the authorized and authenticated session .the owner knows that he has no access to the session any more but is not aware that the attacker has taken over his session and believe that he lost the session due to ordinary lacks in network functioning once the attacker take over a valid session he can use it for various purposes over a certain period of time. These attacks happen in real time.

Replay attack is use to access the network through authorization. The session that is under an attack does not change or disrupts in any way. This does not happen in real time. The attackers get the access to network after the original session expires.

Denial of Service (DoS): an attacker tempers with the data before it is communicated to the sensor node. It causes a denial of service attack due to wrong or misleading information. Jamming is One of DoS attack on network availability. It is a performed by malicious attackers who use other wireless devices to disable the communication of the users in legitimate wireless network.

Dictionary building attacks: In these types of attacks an attacker goes through a list of candidate passwords one by one; the list may be explicitly enumerated or numerated or implicitly defined, can incorporate knowledge about the victim, and can be linguistically derived. Dictionary building attacks are possible after analyzing enough traffic on a busy network.

To avoid these threats and improve the security of the wireless networks various companies collaborated to make the Wi-Fi alliance to make the robust security protocol. Initially they come with the new security protocol for wireless network various companies collaborated to make the Wi-Fi alliance to make the robust security protocol for wireless network known as Wi-Fi protected Access (WPA). The WPA protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate the measure to take the place of WEP. WPA uses the temporal key integration measure to take the place of WEP. WEP uses the Temporal Key Integration Protocol (TKIP) algorithm for encryption. TKIP is security protocol used in the IEE E 802.11i wireless networking standard. TKIP is designed by IEEE802.11i task group and the Wi-Fi alliance as the solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because a the backing the WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for already deployed hardware[2] .

WPA has following advantages:

- A cryptographic Message Integrity Code (MIC), called Michal, to defeat forgeries. Message Integrity Code (MIC) is computed to detect errors in the data contents, either due to transfer errors or due to purposeful alternations. This prevents man in the middle attack, denial of service attack.
- A new Initialization Vector (IV) sequencing discipline, to remove Replay attacks from the attacker`s arsenal.
- A rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. Thus provides security against eavesdropping attacks.

Although WPA protocol has increased wireless security to a great extent but it also has some problems.

- Weakness in passphrase choice in WPA Interface: This weakness on based on Pair Wise Master Key (PMK) that is derived from the concatenation of the passphrase, Service Set Identifier (SSID) , length of the SSID and nonces .
- Possibility of the Brute Force Attack: Brute force is considered to be a passive attack in

which the intruder will generate every possible permutation in the key and try to decrypted the encrypted message with each generated permutation, and validate the output of means of cross comparisons with words, File header any other data.

- Placement of MIC: It is considered a problem because it can be us by any hacker in validating the contents of the decrypted message combined with the brute force attack.

After the WPA new protocol came which is called Wi-Fi Protected Access 2 (WPA2)

The IEEE 802.11i standard also known as Wi-Fi Protected Access 2 (WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on June 24th, 2004, and replaces the previous security specifications, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced as an intermediate solution to WEP insecurities. WPA implemented only a subset of IEEE 802.11i. WPA2 makes use of a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. The use of the Advanced Encryption Standard (AES) is a more secure alternative to the RC4 stream cipher used by WEP and WPA.

3. Wi-Fi Protected Accesses 2

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware. The authentication piece of WPA2 has two modes: Personal and Enterprise. The Personal mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode, which requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol) which offers five EAP standards to choose from: EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), Protected EAP vo/EAP-Microsoft’s Challenge Handshake Authentication Protocol v2 (PEAPvo/EAP-MSCHAPv2), Protected EAP v1/EAP-Generic Token Card (PEAPv1/EAP-GTC) and EAP-Subscriber Identity Module of the Global System of Mobile Communications (EAP-SIM). The Enterprise mode has the following hardware/software implementation requirements:

- Selection of EAP types that will be supported on stations, APs (Access Point), and authentication servers.
- Selection and deployment of authentication servers typically RADIUS (Remote Authentication Dial in User Service) based authentication servers.
- WPA2 software upgrades for APs and clients.

WPA2 establishes a secure communication context in four phases. In the first phase the parties, AP and the client, will agree on the security policy (authentication method, protocol for unicast traffic, protocol for multicast traffic and pre-authentication method) to use that is supported by the AP and the client. In the second phase (applicable to Enterprise mode only)

802.1X authentication are initiated between the AP and the client using the preferred authentication method to generate an MK (common Master Key). In the third phase after a successful authentication, temporary keys (each key has limited lifetime) are created and regularly updated; the overall goal of this phase is key generation and exchange. In the fourth phase all the previously generated keys are used by the CCMP protocol to provide data confidentiality and integrity.

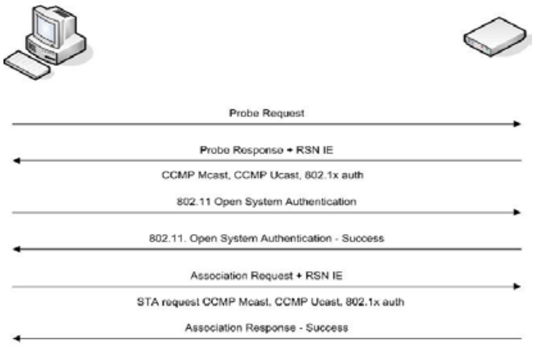

Probe Request
Probe Response + RSN IE
CCMP Mcast, CCMP Ucast, 802.1x auth
802.11 Open System Authentication
802.11. Open System Authentication - Success
Association Request + RSN IE
STA request CCMP Mcast, CCMP Ucast, 802.1x auth
Association Response - Success

Figure 3. Agreeing on the security policy

3.1 WPA2 Authentication

One of the major changes introduced with the WPA2 standard is the separation of user authentication from the enforcement of message integrity and privacy, thereby providing a more scalable and robust security architecture suitable to home networks or corporate networks with equal prowess.

Authentication in the WPA2 Personal mode, which does not require an authentication server, is performed between the client and the AP generating a 256-bit PSK from a plain-text pass phrase (from 8 to 63 characters). The PSK in conjunction with the Service Set Identifier and SSID length form the mathematical basis for the PMK (Pair-wise Master Key) to be used later in key generation. Authentication in the WPA2 Enterprise mode relies on the IEEE 802.1X authentication standard. The major components are the supplicant (client) joining the network, the authenticator (the AP serves as the authenticator) providing access control and the authentication server (RADIUS) making authorization decisions. The authenticator (AP) divides each virtual port into two logical ports, one for service and the other for authentication, making up the PAE (Port Access Entity). The authentication PAE is always open to allow authentication frames through, while the service PAE is only open upon successful authentication by the RADIUS server. The supplicant and the authenticator communicate using Layer 2 EAPoL (EAP over LAN). The authenticator converts EAPoL messages to RADIUS messages and then forwards them to the RADIUS server. The authentication server (RADIUS), which must be compatible with the supplicant's EAP types, receives and processes the authentication request. Once the authentication process is complete the supplicant and authenticator have a secret MK (Master Key) as shown in Figure 4.

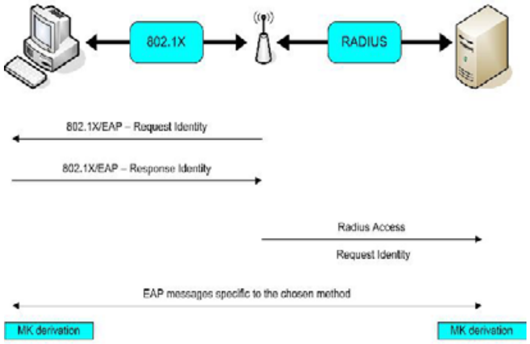

802.1X
RADIUS
802.1X/EAP – Request Identity
802.1X/EAP – Response Identity
Radius Access
Request Identity
EAP messages specific to the chosen method
MK derivation
MK derivation

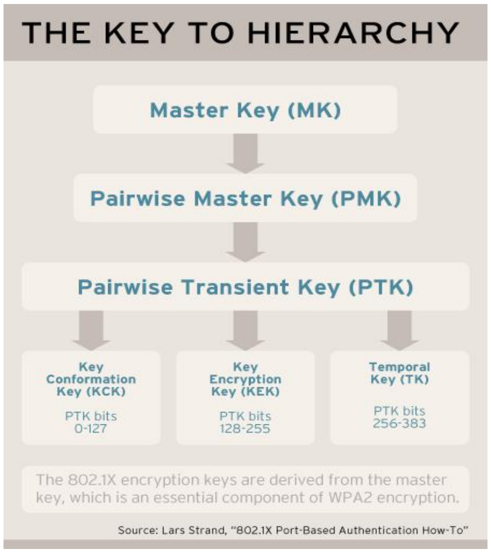
Figure 3.1 802.1X authentication [5]

3.2 WPA2 Key generation

WPA2 key generation is accomplished by means of two handshakes: a 4-Way Handshake for PTK (Pair-wise Transient Key) and GTK (Group Transient Key) derivation, and a Group Key Handshake for GTK renewal.

The 4-Way Handshake, accomplished by four EAPoL-Key messages between the client and the AP, is initiated by the access point and performs the following tasks:

- Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is dependent on the authentication
- Method used. In WPA2 Personal mode the PMK is derived from the authentication PSK and for WPA2 Enterprise mode the PMK is derived from the authentication MK (key hierarchy in Figure 3).
- Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, KEK (Key Encryption Key – 128 bits) used to encrypt the GTK and the TK (Temporal Keys – 128 bits) used to secure data traffic.
- Install encryption and integrity keys.
- Encrypt transport of the GTK which is calculated by the AP from a random GMK (Group Master Key).
- Confirm the cipher suite selection



The 802.1X encryption keys are derived from the master key, which is an essential component of WPA2 encryption.

Source: Lars Strand, "802.1X Port-Based Authentication How-To"

Figure 3.2 MK hierarchy [16] [5]

The Group Key Handshake is only used to disassociate a host or renew the GTK and uses the KEK generated during the 4-Way Handshake to encrypt the GTK.

3.3 WPA2 Encryption

The AES used by WPA2 “is a block cipher, a type of symmetric key cipher that uses groups of bits of a fixed length – called blocks” [13]. A symmetric key cipher is a set of instructions or algorithm that uses the same key for both encryption and decryption. In the WPA2/802.11.i implementation of AES, bits are encrypted (using a 128 bit key length) in blocks of plaintext, that are calculated independently, rather than a key stream acting across a plaintext data input stream. AES encryption includes 4 stages that make up one round and each round is iterated 10 times.

AES uses the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication (with different initialization vectors). The two underlying modes employed in CCM include Counter mode (CTR) , that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

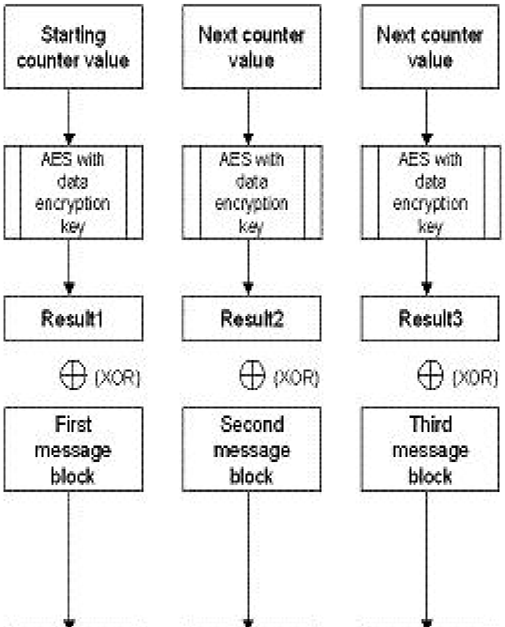


Figure 3.3 AES Counter Mode [11]

CBC-MAC is used to generate an authentication component as a result of the encryption process (Figure 5). This is different from prior Message Integrity Code (MIC) implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 128-bit Initialization Vector (IV).

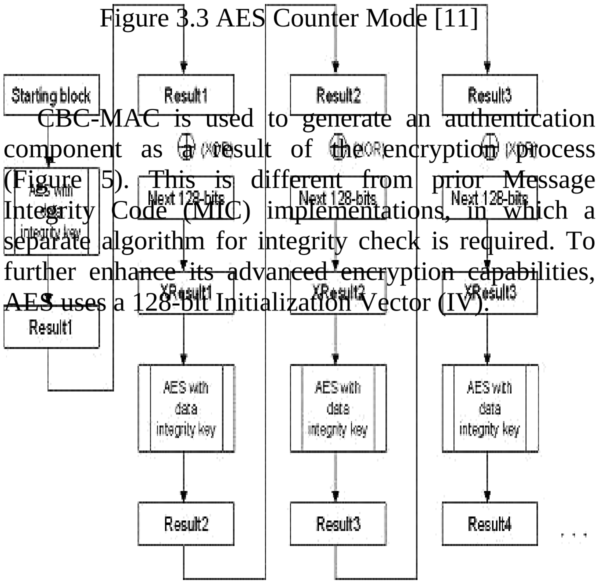


Figure 3.3.1 AES CBC-MAC [11]

3.4 WPA2 Encryption Steps

The MIC - similar to a checksum - provides data integrity for the non changeable fields in the 802.11 header, unlike WEP and WPA, preventing packet replay from being exploited to decrypt the package or compromise cryptographic information. The MIC is calculated using a 128-bit IV as follows:

IV is encrypted with AES and TK to produce a 128-bit result.

128-bit result is XOR with the next 128 bits of data.

The result of XOR is then passed through steps 1 and 2 until all 128 blocks in the 802.11 payload are exhausted.

At the end of the operation the first 64 bits are used to produce the MIC.

The Counter Mode algorithm encrypts the data and the MIC (calculated using the CBC-MAC). The Counter Mode algorithm begins with a 128-bit counter preload similar to the MIC IV, but uses a counter value initialized to 1 instead of a data length resulting in a different counter used to encrypt each packet. The data and the MIC are encrypted as follows:

Initialize counter if it is the first time otherwise increment counter.

First 128 bits are encrypted using AES and TK to produce a 128-bit result.

A XOR is performed on the result of step 1.

The first 128 bits of data produce the first 128-bit encrypted block.

Repeat steps 1-4 until all the 128-bit blocks have been encrypted.

Set counter to zero and encrypt it using AES and XOR with MIC appending the result the encrypted frame.

3.5 Benefits of WPA2

WPA2 (along with WPA) resolved vulnerabilities of WEP to “hacker attacks such as ‘man-in-the-middle’, authentication forging, replay, key collision, weak keys, packet forging, and ‘brute–force/dictionary’ attacks”[13]. By using government grade AES encryption and 802.1X/EAP authentication WPA2 further enhances the improvements of WPA using TKIP encryption and 802.1X/EAP authentication over WEP’s imperfect encryption key implementation and its lack of authentication. “AES has no known attacks and the current analysis indicates that it takes 2120 operations to break an AES key”[13].

In addition to the encryption benefits, WPA2 also adds two enhancements to support fast roaming of wireless clients moving between wireless AP’s.

PMK caching support – allows for reconnections to AP’s that the client has recently been connected without the need to re-authenticate.

Pre-authentication support – allows a client to pre-authenticate with an AP towards which it is moving while still maintaining a connection to the AP it’s moving away from.

PMK caching support and Pre-authentication support enable WPA2 to reduce the roaming time from over a second to less than 1/10th of a second. The ultimate benefit of the fast roaming is that WPA2 can now support timing-sensitive applications like Citrix, video, or VoiP (Voice over IP) which would break without it.

4. Literature Review

The Kirti Raj Bhatele,[3] presented hybrid security protocol for better security using a combination of both symmetric and Asymmetric cryptographic Algorithms. In this hash value of the decrypted message using AES algorithm is calculated using MD5 algorithm. This hash value has been encrypted with dual RSA and the encrypted message of this hash value also sent to destination. Now at the receiving end, hash value of decrypted plaintext is calculated with MD5 and then it is compared with the hash value of original plaintext which is calculated at the sending end of its integrity. By this we are able to know whether the original text being altered or not during transmission in the communication medium.

Arash Habibi Lashkari,[4] presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocols types, weaknesses and enhancements, WPA protocols types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problem on WPA that happened on PSK part of algorithm. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

Gamal Selim,[5] explained various types of security attacks modification, fabrication, interception, brute force, maintainability, and static placement of MIC. They surveyed currently available security protocols that are WEP, WEP2 and WPA2. They also proposed a new mechanism called multiple slot system (MSS). MSS make use of the key selector, slot selector and MIC shuffle selector, MSS uses one of four encryption algorithm RC4, RSA, Blowfish and AES.

LifenSang,[7] Shared secret free security infrastructure for wireless networks based on two physical primitives. Cooperative jamming and spatial signal enforcement- Cooperative jamming is for confidential wireless communication and spatial signal enforcement is for message authenticity. Proposed infrastructure provides confidentiality, identity, authentication, message authentication, integrity, non-repudiation, receiver non repudiation anonymity.

Andew Gin,[8]Compared the performance analysis of evolving wireless 802.11security architecture. Paper explained wireless network security methods. Paper explain security layers like WEP shared key authentication and 40 bit in encryption WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption ,WPA with EAP –TLS authentication RC4 encryption , WPA2 with PSK authentication and AES encryption and WPA2 with EAP –TLS authentication and AES encryption. Effects on Throughput are also disused.

Floriano De Rango,[9] Proposed static and dynamic 4-way handshake solutions to avoid denial servicer attack in WPA and IEE 802.11i. Paper also explained DoS and DoS flooding attack against IEE802.11i 4-way handshake.

5. Summary

Security is the major concern in Wireless Network. To prevent the wireless security threats various technologies has been evolved. The security threats come from vulnerabilities in the security protocols such as Traffic analysis, Eavesdropping, Unauthorized Access. To provide the secure wireless communication for organizations and individuals is always the main goal of all security protocols and hence WEP, WAP and WAP2 are evolved. At present WPA2 is the most secure technique used in wireless communication which comes under IEEE802.11i specification. WPA2 is the advanced version of Wi-Fi Protected Access (WPA). WPA2 makes use of a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP). WPA2 (along with WPA) resolved vulnerabilities of WEP to hacker attacks it shows that this technique is fine for wireless network security up to 2120. WPA2 also have some vulnerability which is in physical layer. To prevent the attacks in physical layer quite difficult, however some solutions have been suggested such as by dynamically adjusting the RF power level. Operational security measures such as site surveillance, as well as planning the Wi-Fi RF coverage area.

6. References

[1] S.D.Kanawat and P.s. Parihar,Editors, “Attacks in Wireless Networks”, International jornal of Saart Sensors amd Adhoc Networks,(2011) May 18-23

[2] Y.X.Lim and T.SChmoyer, “Editors,Wireless Intrusion Detection and response”, IEEE Information Assurance Workshop,(2003) June18-20,westpoint,New York

[3]A.Sinhal and M.Pathak,Editors, “A Novel Approach to the Design of New Hybrid Security rotocol Architecture”, IEEE international Conference on Advanced Communication Control and Computing Technologies(ICACCCT),(2012) August 23 Ramanadhapuram.

[4] A.H.Lashkari and M.M.S. Danesh, Editors, “A Survey on Wireless Security Protocols, WEP, WPA and WPA2/802.11i”,IEEE international Conference on Computer Science and Information Technology,(2009) august 8-11 Beijing.

[5]G.Selim, H.M.E. Badawy and M.A. Salam, Editors, “New Protocol Design For Wireless Network Security”, IEEE international Conference on Computer Science and Information Technology, (ICACT), (2006) feb 20-22 .

[6] H.W.Lee, A.S.K. Pathan and C.S. Hong Editors, “Security in Wireless Sensor Networks, Issues and Challenges”, international Conference on Advanced Communication Technology (ICACT) (2006) feb 20-22 phoenix park.

[7] L.Sang andA.Arora Editors, “A Shared Secret Free Security Infrastructure For Wireless Network”, ACM Transactions on Autonomous and Adaptive System (TAAS) (2012) July

[8] A.Gin and R. Hunt, Editors, “Performance Analysis Of Evolving Wireless IEEE 802.11 security Architectures”, ACM international Conference on Mobile Technology Application and Systems (2008)

[9] F.De Rango , D.C.Lenti ans S.Marano, Editors, “Static and Dynamic Four way handshake Solution to avoid Denial of Service Attack in Wi-Fi Protected access and IEEE 802.11i”,EURASIP, Journal on wireless Communication and Networking (2006) June

[10]"IEEE 802.11i." Wikipedia, The Free Encyclopedia. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006

[11]“Wi-Fi Protected Access 2 Data Encryption and

Integrity.” Microsoft TechNet. The Cable Guy. July 29 2005.

[12]“Understanding the updated WPA and WPA2 standards”. ZDNet Blogs.PostedbyGeorge Ou. June 2 2005.

[13]“Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise.” Wi-Fi Alliance, Feb. 27 2005

[14]Lehembre, Guillaume. “Wi-Fi security –WEP, WPA and WPA2”. Article published in number 1/2006 (14) of hakin9, Jan. 2006. Publication on www.hsc.fr on Dec. 28 2005.

[14]Ou, George. “Wireless LAN security guide”. www.lanarchitect.net. Revision 2.0 Jan 3 2005

[15]Bulk, Frank. “Learn the basics of WPA2 Wi-Fi security”. Network Computing Jan. 27 2006.

"Extensible Authentication Protocol." Wikipedia, The Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation, Inc. Nov 27 2006

[16]Gupta, Ashok and Buthmann, Theresa. “The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security”. Lucent Technologies Sep. 11 2006 (15).