International Journal of Civil Engineering and Technology (IJCIET)
Volume 8, Issue 8, August 2017, pp. 841–851, Article ID: IJCIET_08_08_087
Available online at http://http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=8&IType=8
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

SECURITY FOR WIRELESS LOCAL AREA NETWORK WITH PRE SHARE KEY AUTHENTICATION USING WI-FI PROTECTED ACCESS

Paparao Nalajala
Dept. of Electronics and Communication Engineering,
Institute of Aeronautical Engineering, Hyderabad, India

Dr. R. V. Krishnaiah
Dept. of Electronics and Communication Engineering,
Institute of Aeronautical Engineering, Hyderabad, India

B Annapurna
Dept. of Electronics and Communication Engineering,
MLR Institute of Technology, Hyderabad, India

Bhavana Godavarthi
Dept. of Electronics and Communication Engineering,
Institute of Aeronautical Engineering, Hyderabad, India

ABSTRACT

Wireless Local Area Networks (WLANs) have become very popular due to their high data rates, cost effectiveness, flexibility and ease of use. On the other hand, they are facing major security threats due to the broadcast nature of the wireless media. 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 to avoid these threats using the Wi-Fi Protected Access 2 (WPA2) protocol used to secure communications in Wireless Networks. It differs from the other solutions because it works in the three WLAN security levels. WEP/WPA2 encryption, AES, and strong 802.1x authentication are integrated into the solution to provide a high level of security against threats.

Key word: Linux system, 802.1x, WLAN Access point, Network interface card, Wi-Fi Device.

Cite this Article: Paparao Nalajala, Dr. R. V. Krishnaiah, B Annapurna and Bhavana Godavarthi, Security For Wireless Local Area Network with Pre Share Key Authentication Using Wi-Fi Protected Access, International Journal of Civil Engineering and Technology, 8(8), 2017, pp. 841–851.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=8&IType=8

1. INTRODUCTION

WLANs are considered of the most popular networks technologies today. Both individuals and large companies are using them due to their advantages WLANs popularity came from their advantages such as flexibility, mobility, easy installation and low cost relative to wired networks [1]. Despite all these advantages, there is a major problem that related to its security. While the data transmitted over wireless media can be accessed anywhere with minimal infrastructure cost, the violation of the wireless LANs security is automatically being harmful to wired LAN. Once the data is transmitted over the wireless media, then there is a chance of security attack [2] A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive Information over the air. Wireless LAN is very popular nowadays. Wireless local area networks enable users to communicate without the need of cable. Below is an example of a simple WLAN the major difference between wired LAN and WLAN is WLAN transmits data by radiating energy waves, called radio frequency waves, instead of transmitting electrical signals over a cable IEEE 802.11 is a standard specification for implementing wireless local area network. Computer communication [2] [3] in the 2.4, and 5GHZ frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. Apart from the above the latest technologies like 802.11ac and 802.11ad provides up to 7Gbit/s which requires Gigabit switches and advanced hardware[4] [5].

There are three wireless security mechanisms for achieving these standard security requirements.

1. Strong encryption is used to provide strong Confidentiality and integrity for data.
2. Checksum/hash algorithms are used to provide integrity protection and authentication.
3. Strong authentication is used for strong access control and nonrepudiation.

Our main goal is to achieve a more secure and reliable WLAN. There are many security solutions such as WEP, WPA, WPA2 and WPA2 with different 802.1x RADIUS servers. Each security solution has to provide the standard security requirements to make a secure WLAN. Most of the studies [5&6&7] in the WLAN security have been done at one level 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. 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.

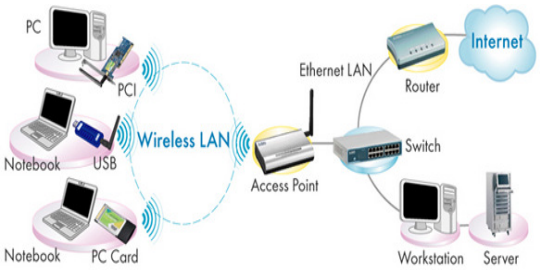

Figure 1 Wireless Communication

2. EXISTING WLAN SECURITY SOLUTIONS

There are different security solutions for the IEEE 802.11 standard like Wired Equivalent Protocol (WEP), WPA, WPA2, and WPA2 using 802.1x servers. We explain the detail of each solution in the following:

WEP is the first security technique used in IEEE 802.11 standards and it provides security level for the WLANs equals to the wired LAN. WEP helps to make the communication secure and provides secret authentication scheme between the AP and the end user. WEP is implemented on initial Wi-Fi networks where the user cannot access the network without the correct key [9]. WEP uses the shared key authentication method in which the user needs two things to access the WLANs, the service set identifier (SSID) and the WEP key generated by the AP.

2.1. Wi-Fi Protected Access (WPA)/ Temporal

Key Integrity Protocol (TKIP) There is a need to develop a new solution for WLANs security that provides more security than WEP. TKIP is designed on top of WEP to fix all its known weaknesses. To increase the key ability of WEP, TKIP includes four additional algorithms.

WPA2 / Advanced Encryption Standard (AES):

AES is created by the American Institute of National Standards and Technology (NIST) in 2001 and it is considered as the best specification for data encryption. It based on Rijndael's cipher, which is developed by two cryptographers, Joan Daemon, and Vincent Rijmen, who submitted the proposal which evaluated by NIST during the selection process AES. WPA2 structure is different from WPA and WEP because the ingredients single key management and message integrity, CCMP, based on AES.

The purposes of AES (CCMP) encryption are

1. Counter mode is used for providing data protection from unauthorized access.
2. CBC-MAC is used to provide the message integrity to the network.

2.2. Wireless Local Area Network (Wlan)

One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters [2] [3].

A. Access Points

Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. An AP operates within a specific frequency spectrum and uses

802.11standard Specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

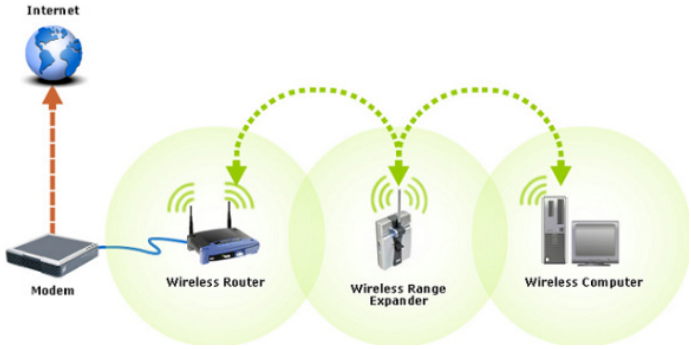

Figure 2 Linksys Wireless Access point

2.3. WLAN Security

There are two types of WLAN architecture: Independent or Adhoc mode and infrastructure mode WLAN [4] [5].

A. Independent WLAN

The simplest WLAN configuration is an independent (or peer- to-peer) WLAN. It is a group of computers, each equipped with one wireless LANNIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. Independent networks can be set up whenever two or more wireless adapters are within range of each other

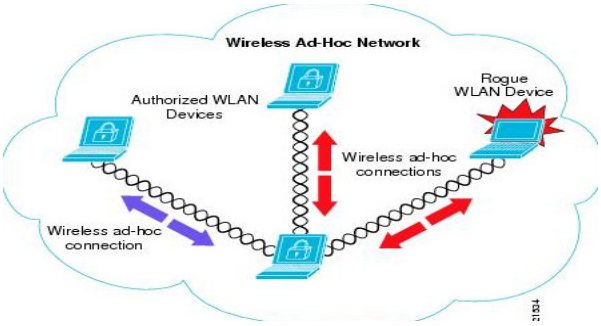

Figure 3 Independent WLAN or ADHOC Mode WLAN

B. Infrastructure WLAN

Infrastructure WLAN consists of wireless stations and access points. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighborhood. This network configuration satisfies the need of large-scale networks arbitrary coverage size and complexities.

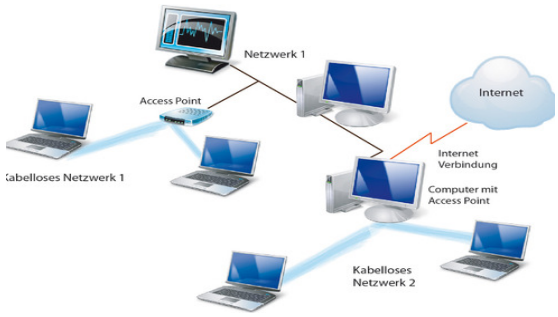

Figure 3.1 Infrastructures WLAN

A. Security Threats of WLAN

Despite the productivity, convenience and cost advantage that WLAN [2] [6] offers, the radio waves used in wireless networks create a risk where the network can be hacked. This section explains three examples of important threats: Denial of Service, Spoofing, and Eavesdropping.

B. Denial of Service

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN [1] [3] can easily be overwhelmed and leave them open to denial of service attacks.

C. Spoofing and Session Hijacking

This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 do not require an access point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN [3].

D. Eavesdropping

This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.

3. WIRELESSSECURITIES

3.1. Wired Equivalent Privacy (WEP)

WEP is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats. Basically, WEP [10][16] provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information. The following section explains the technical functionality of WEP as the main security protocol for WLAN.

3.2. How WEP Works

When deploying WLAN, it is important to understand the ability of WEP [10] to improve security. This section describes how WEP functions accomplish the level of privacy as in a wired LAN WEP uses a pre-established shared secret key called the base key, the RC4encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks. WEP [16] supports up to four different base keys, identified by Key IDs 0 thorough 3. Each of these base keys is a group key called a default key, meaning that the base keys are shared among all the members of a particular wireless network. However, this is less common in first generation products, because it implies the existence of a key management facility, which WEP does not define. The WEP specification does not permit the use of both key-mapping keys and default keys simultaneously, and most deployments share a single default key across all of the802.11devices.

WEP tries to achieve its security goal in a very simple way. It operates on MAC protocol Data Units (MPDUs), the 802.11 packet fragments. To protect the data in an MPDU, WEP first computes an integrity check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP appends the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to detect if data has been corrupted in flight or the packet is an outright forgery. Next, WEP selects a base key and an initialization vector (IV), which is a 24- bit value. WEP constructs a per-packet RC4 key by concatenating the IV value and the selected shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and Key ID identifying the selected key is encoded as a four-byte string and pre-pended to the encrypted data. Figure 4depicts a WEP-encoded MPDU.

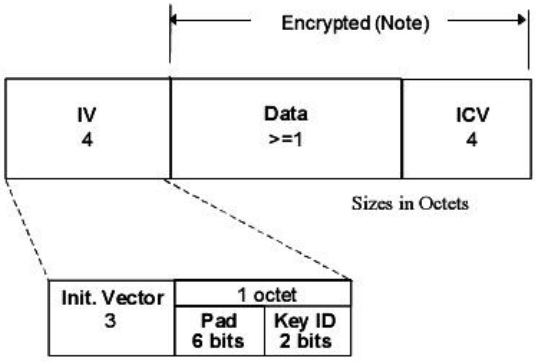

Figure 4 WEP-encoded MPDU

3.3. Wi-Fi Protected Access (WPA)

To overcome the limitations of WEP [10][16] the WPA came into existence. WPA is the subset of the IEEE's 802.11i wireless security specification. Temporal Key Integrity protocol (TKIP) is the encryption method of WPA. The weaknesses of WEP addresses by TKIP by including mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. The radius is to authenticate each server, WPA which depends upon central authentication. The compatible version of IEEE 802.11i is WPA, which is under development. To implement WPA both server and client computers updates their software's during 2003.WEP/WPA modes access points can operate to support both WEP and WPA clients. WEP security level is compatible with mixed level security for all users. The password will trigger authentication and TKIP encryption.

3.4. WPA-802.1x and WPA-PSK

WPA comes in two flavors that is WPA-802.1 x [7] and WPA-PSK. WPA-802.1x is a good choice for large businesses because it combines access point authentication with another layer of authentication through external authentication services. This means that after the authenticating user associates with the wireless access point, his or her credentials are also checked against a locally stored database or even external sources (for example RADIUS or Kerberos). Authentication servers also distribute security keys to individual users dynamically. WPA-PSK on the other hand is a solution for small businesses and homes which utilizes so-called Pre-Shared Key (PSK) which is technically (from the user perspective) similar to how security keys with WEP are implemented but in a more secure way (more about this in the TKIP section below).

As the name suggests, WPA2 is a second, newer version of Wireless Protected Access (WPA) security and access control technology for Wi-Fi wireless networking. WPA2 [5] is available on all certified Wi-Fi hardware since 2006 and was an optional feature on some products before that. It is designed to improve the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires.

Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations). Most wireless routers for home networks support both WPA and WPA2 and administrators must choose which one to run. Obviously, WPA2 is the simpler, safer choice. Some techies point out that using WPA2 requires Wi-Fi hardware to work harder in running the more advanced encryption algorithms, which can theoretically slow down the network's overall performance compared to running WPA. Network owners can make their own choice but should run experiments to decide whether they notice any difference in their networks speeds with WPA2 vs. WPA Encryption algorithm and security fundamentals

WPA employs the RC4 encryption [9] mechanism which is the same like WEP, but WPA uses a longer security key, 128 bit in length (compared to 104 bit in WEP) and longer initialization vector, 48 bit in length (compared to 24 bit in WEP). This gives WPA more strength compared to WEP because a hacker would need to capture significantly more data packets in case of WPA when trying to perform so-called statistical attack.

A. Encryption algorithms inWPA2

WPA2 compliments TKIP and the improved data integrity control algorithm with more secured encryption mechanism called Advanced Encryption Standard (AES) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). In other words, this means an improved encryption algorithm. Experts say that AES-CCMP is robust enough to be used for government data security purposes.

B. New Standards for Improving WLAN Security

Apart from all of the actions in minimizing attacks to WLAN [2] mentioned in the previous section, we will also look at some new standards that intend to improve the security of WLAN. There are two important standards that will be discussed in this paper: 802.1x and 802.11i [6][7]. IEEE 802.1x relates to EAP in a way that it is a standard for carrying EAP over a wired LAN or WLAN. There are four important entities that explain this standard

I. Authenticator

Authenticator is the entity that requires the entity on the other end of the link to be authenticated. An example is wireless access points.

II. Supplicant

Supplicant is the entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.

I. Port Access Entity (PAE)

It is the protocol entity associated with a port. It may support the functionality of Authenticator, Supplicant or both.

II. Authentication Server

Authentication server is an entity that provides authentication service to the Authenticator. It may be co-located with Authenticator, but it is most likely an external server. It is typically a RADIUS (Remote Access Dial in User Service) server. The supplicant and authentication server are the major parts of 802.1xs.

4. 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)

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

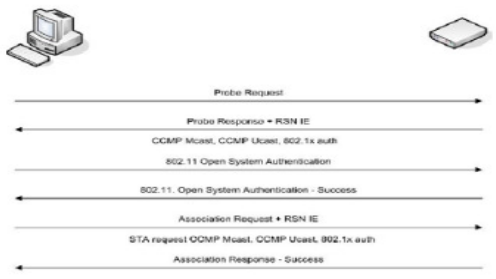

Figure 5 Agreeing on the security policy

4.1. 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 keygeneration. Authentication in the WPA2 Enterprise mode relies on the IEEE 802.1Xauthentication 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.

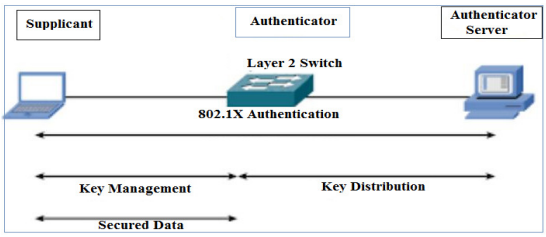

Figure 6 General topology of 802.1x Authentication

5. RESULT

Security settings in wireless router/access point shown the below figure.

Figure 6.1 Security settings in wireless router/access point

Finally, bind the access point with the authentication Server by Radius password (that falls in the same network), as shown below figure.

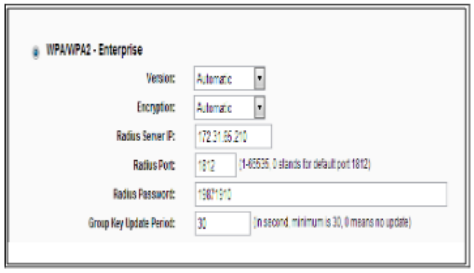

Figure 7 Binding the access point with the Free RADIUS server

6. APPLICATIONS

Applications of wireless communication involves in Computer devices like Laptops, Smart Phones, Tablets, Notebooks, unity systems, television remote control, Wi-Fi, Cell phones, Computer interface devices and various wireless communication based projects.

7. CONCLUSIONS

The development of wireless network is the unique and outstanding in the technology world because of its various advantages, portability and convenient to end user. But security is the main concern, without implementation of security features in wireless network result data network hacking and data will be infected by some malicious virus or Trojan horses. So to avoid this huge loss we need to use security features like WEP, WPA,WPA2 algorithms and while configuring wireless router or wireless access point. Apart from the above algorithms we need to implement few incorporate access control Features such as MAC address filtering that deny requests from unwanted clients and also basic security precautions

8. FUTURE SCOPE

Wireless technology development is growing rapidly and usage of wireless network among the people growing because of its convenience and faster working. Now days without wireless network we can't imagine this new generation. But as the Wi-Fi users are growing day-by-day there is a need to increase data rates and also high frequency bandwidth devices recently a new technology has been introduced and made the wireless technology more advance, named as the Wireless Gigabit technology or WIGIG. Basically it is defined as the wireless technology that operates wireless over 60 Hz frequency band is called as the WIGIG technology. This technology is designed for the sake of the faster communication and faster transmission of data from one place to another at the more speed then Wi-Fi or the wireless LAN.

ACKNOWLEDGEMENT

I have taken efforts in this project. The authors would like to thanks however, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

REFERENCES

[1] F. Sheldon, J. Weber, S. Yoo, W. Pan, The Insecurity of Wireless Networks, IEEE Computer Society, 10(4), July/August, 2012, pp. 54-61.

[2] S .Deepthi G Mary Swarnalatha, Paparao Nalajala, Wireless Local Area Network Security Using Wpa2-Psk, International journal of advanced trends in computer science and engineering, Volume V, Issue I, Jan 2016, pp. 41-45.

[3] L. Wang, B. Srinivasan, N. Bhattacharjee, Security Analysis and Improvements on WLANs, Journal of Networks, 6(3), March 2011, pp.470-481.

[4] P. Feng, Wireless LAN Security Issues and Solutions, IEEE Symposium on Robotics and Applications, KualaLumpur,Malaysia,3-5 June, 2012, pp.921-924.

[5] H. Bulbul, I. Batmaz, M. Ozel, Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security

[6] M. Mathews, R. Hunt, Evolution of wireless LAN security architecture to IEEE802.11i (WPA2),University of Canter bury, New Zealand

[7] 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.

[8] S. K. Asagodu, Wireless *LAN Security and IEEE 802.11 Department* of Computer Science Engineering: Vishveshwaraiah Technological University- S.D.M College of Engineering and Technology, 2009-10.

[9] Wi-Fi Protected Access 2 Data Encryption and Integrity. Microsoft TechNet. The Cable Guy. July 292005.

[10] 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. 282005.

[11] ANSI/IEEE STD 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[12] Kevin Tyrrell, An over view of Wireless security issues, GSEC V1.4b SANS Institute 2003 Stanley Wong, The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards.

[13] Wireless LAN Technologies, http://sourcedaddy.com/networking/wireless-lan-applications.html

[14] K. Hole, E. Dyrnes, P. Thorsheim, P., Securing Wi-Fi Networks, IEEE Computer Society, 2005, 38(7), pp.28-34.

[15] H. Bulbul, I. Batmaz, M. Ozel, Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.

[16] P. Ye &G. Yue, Security Research on WEP of WLAN,*2nd International Symposium on Networking and Network Security (ISNNS'10) Proc.*, Jinggangshan, PR China, 2010.

[17] Prof. Darshan Chauhan and Prof.Dhaval Jadhav, Boost Wi-Fi Router Signal Strength Using Beverage Can, Volume 4, Issue 4, July-August (2013), pp. 122-127, International Journal of Computer Engineering and Technology.

[18] Nilesh P. Bodne and Prof. A .A. Kelkar, VHDL Modeling For Wi-Fi Mac Layer Transmitter and Receiver, Volume 3, Issue 1, January- June (2012), pp. 171-177, International Journal of Electronics and Communication Engineering & Technology.

[19] Dr.A.M. Bhavikatti and Mallikarjun.Mugali, VHDL Modeling of The SRAM Module and State Machine Controller (SMC) Module of Rc4 Stream Cipher Algorithm For Wi-Fi Encryption, Volume 6, Issue 1, January (2015), pp. 79-85. International Journal of Electronics and Communication Engineering & Technology.

[20] F. DeRango, D.C.Lentians S.Marano, Editors, Static and Dynamic Four way handshake Solution to avoid Denial of Service Attack in Wi-Fi Protected access and IEEE802.11i EURASIP, Journal on wireless Communication and Networking (2006) June.