WIFI SECURITY

Mojtaba Mohi Eldeen Adam[1], Ashraf Gasim Elsid Abdallah[2]
[1]*Neelain university department of electronics and communication engineer Khartoum-Sudan*
(E-mail: mojtaba70@hotmail.com; ieeemail70@gmail.com)
[2]*School of Electronics, College of Engineering, Sudan University of Science and Technology, Khartoum, Sudan*
(E-mail: ashrafgasim@sustech.edu ; agea33@hotmail.com; agea33@yahoo.com)

Abstract: *Wireless technology provides us many benefits like portability and flexibility, increased productivity, and lower installation costs. Wi-Fi networks can be accessed with laptops, mobile phones, cameras, game consoles, and an increasing number of other consumer electronic devices. Wireless technologies have become increasingly popular everyday in business as well as in personal lives. Wireless Networking changed completely the way people communicate and share information by eliminating the boundaries of distance and location. In this paper we are discussing about the wireless network challenges and IEEE 802.11 Standards and WEP protocol. in this paper we discussed wireless network ieee802.11standard based in security, three types of security protocols and Security Threats to Wireless Networks was discussed.*

Keywords: *WI-FI, WEP, WPA, WPA.*

---

1. Introduction

Wi-Fi is the name of the popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connection. The Wi-Fi alliance, the organization that owns the wi-fi (registered trade mark) term specifically defines Wi-Fi as any ―wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case.[1][2] Wi-Fi is simply a trademarked term meaning IEEE 802.11x. Initially, Wi-Fi was used in place of only the 2.4GHz 802.11b standard, however the Wi-Fi Alliance has expanded the generic use of the Wi-Fi term to include any type of network or WLAN product based on any of the 802.11 standards, including 802.11b, 802.11a, dual-band, and so on, in an attempt to stop confusion about wireless LAN interoperability.[3] Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.[4] Wi-Fi is supported by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified" and indicates the radio frequency band used (2.5GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).[5]

2. How Wi-Fi Works

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called WiFi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time:

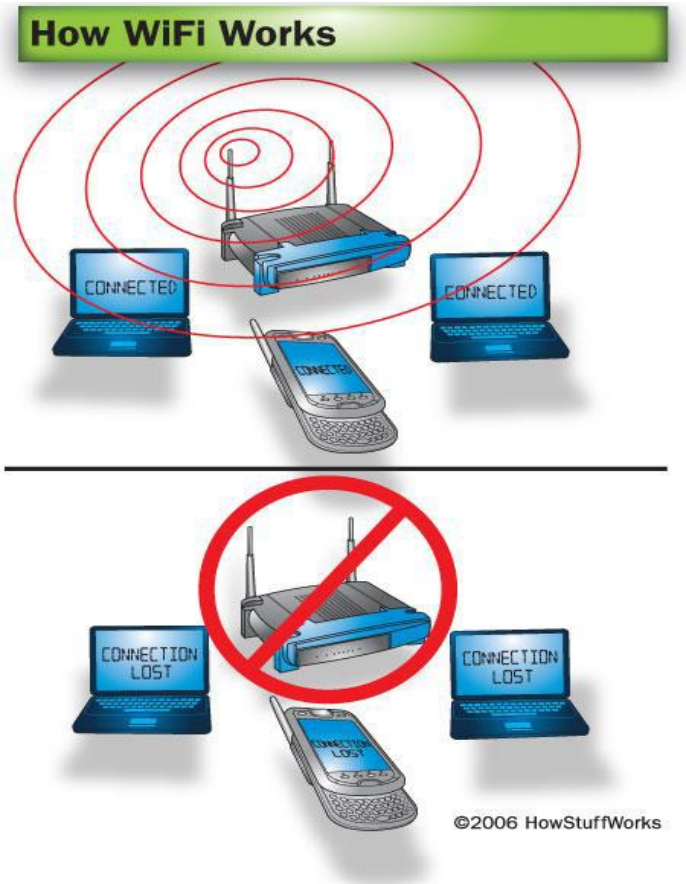

Figure 1. How wifi work

3. IEEE 802.11 Standards

In 1997, IEEE ratified the 802.11 standard for WLANs. The IEEE 802.11 standard supports three transmission methods, including radio transmission within the 2.4 GHz band. In 1999, IEEE ratified two amendments to the 802.11 standard 802.11a and 802.11b that define radio transmission methods, and WLAN equipment based on IEEE 802.11b quickly became the dominant wireless technology [6]. IEEE 802.11b equipment transmits in the 2.4 GHz band, offering data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance, throughput, and security features comparable to wired LANs. In 2003, IEEE released the 802.11g amendment, which specifies a radio transmission method that uses the 2.4 GHz band and can support data rates of up to 54 Mbps. Additionally, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products.[7].

Table 1: compares the different IEEE 802.11 standards:[8]

	802.11A	802.11B	802.11G	802.11N
Date of standard approval	July 1999	July 1999	June 2003	Oct 2009
Maximum data rate (Mbps)	54	11	54	~600
Modulation	OFDM	CCK or DSSS	CCK, DSSS, or OFDM	CCK, DSSS, or OFDM
RF Band (GHz)	5	2.4	2.4	2.4 or 5
Number of spatial streams	1	1	1	1, 2, 3, or 4
Channel width (MHz) nominal	20	20	20	20, or 40

4. 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 [9]. Different types of security attacks are shown in the Figure.

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 important to the attacker is identification and physical location of access point in its surroundings. The third type of information an attacker can get by traffic analysis is information about the communication protocol. An attacker needs to gather the information about the size and 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 used to watch over an unlimited wireless session. The only condition to be fulfilled is that the attacker has the access to the area of emission. With a decrypted session the attacker is able to read the data during its transmission and gather data indirectly by surveying the packages. This kind of attack is not based on violation of privacy but information gathered in this way can be used for more dangerous kinds of attacks.

In Active eavesdropping with partially known plaintext type of attack, the attacker watches over a wireless session and actively injects own messages in order to reveal the content of the messages in the session. Precondition for this type of attack is an access to communication area and some knowledge on the part of the message, such as IP address. The attacker is able to modify the content of the package so that the integrity of the message remains preserved. Usually the attacker changes final IP or TCP address.

In active eavesdropping with known plaintext type of attack, the attacker injects messages known only to him into the traffic in order to create conditions for decryption of the packages that should be received by other wireless users. These conditions are created by creation of Initialization Vector (IV) sequence and message for each single message that is sent. After some time, when a package with the same IV as in database appears, the attacker is able to decrypt the message. The only way to prevent this kind of attacks is to change key often.

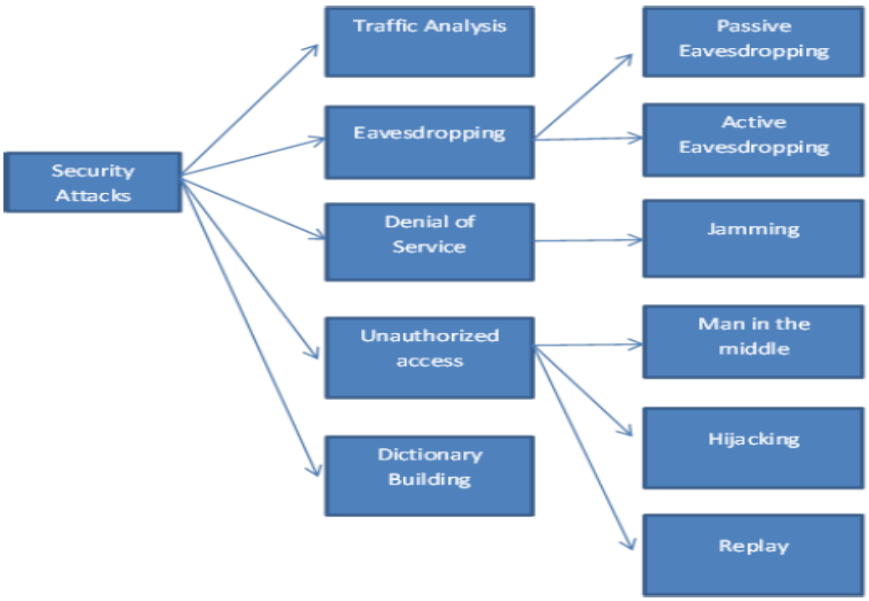

Figure 2. Different Types of Security Attacks

Unauthorized access: Once the attacker gets the access to the network, he is able to initiate some other types of attacks or use network without being noticed. Some can be of an opinion that unauthorized use of the network is not a significant threat to the network since the access rights allocated to resources will disable the attackers. However, usually the unauthorized access is the key to initialization of ARP (Address Resolution Protocol) attack. Virtual Private Network (VPN) and IPsec solution can protect users from the attacks that directly influence the confidentiality of application data but cannot prevent attacks that indirectly ruin confidentiality. Man in the middle, high-jacking and replay attacks are the best examples of these kinds of attacks

Man in the middle attack enables data reading from the session or modifications of the packages with violate integrity of the session. There are several ways to implement this type of attack. One way is when attacker disrupts the session and does not allow for the station to establish communications again with the Access Point (AP). Station tries to establish session with the wireless network through AP, but can do that only through the workstation of the attacker pretending to be AP. At the same time, the attacker establishes connection and authentication with the AP. Now there are two encrypted tunnels instead of one: one is established between the attacker and AP, while the second one is established between the attacker and the station. This enables attacker to have the access to the data exchanged between the working station and the rest of the network. ARP attack is a sub-type of the man in the middle attack since these attacks are directed towards one component of wired network and not towards wireless clients. The attacker escapes authentication or provides false accreditations by this kind of attack. The attacker becomes valid user and gets the access to the network as authenticated user by getting the false accreditations.

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 believes that he lost the session due to ordinary lacks in network functioning. Once the attacker takes over a valid session he can use it for various purposes over a certain period of time. This attack happens in a real time.

Replay attack is used to access the network through authorization. The session that is under an attack does not change nor disrupt in any way. The attack does not happen in a real time. The attacker gets the access to the network after the original session expires. The attacker comes to the authentication of one or more sessions, and then replies to the session after a certain period of time or uses couple of sessions to compose the authentication and reply to it.

Denial of Service (DoS): An attacker tampers with the data before it is communicated to the sensor node. It causes denial of service attack due to wrong or misleading information. Jamming is one of DoS attack on network availability. It is performed by malicious attackers who use other wireless devices to disable the communications of users in a 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 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 to improve the security of the wireless networks various companies collaborated to make the Wi-Fi alliance to make the robust security protocol. Initially they came with the new security protocol for wireless networks as following:

A. WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is a security mechanism for Wireless LAN. It was introduced in September 1999 as part of IEEE 802.11 security standard.

The purpose of Wired Equivalent Privacy (WEP) was to provide security comparable to that of wired networks. RC4 stream cipher is used by WEP to provide confidentiality and CRC-32 for data integrity [10].

The standard specified for WEP provides support for 40 bit key only but non standard extensions have been provided by various vendors which provide support for key length of 128 and 256 bits as well. A 24 bit value known as initialization vector is also used by WEP for initialization of the cryptographic key stream.

I. WEP Encryption/Decryption Process

WEP Encryption process consists of following steps:

i. 24 bit initialization vector is concatenated with 40 bit WEP key.

ii. The resultant concatenated key acts as seed value for Pseudo random number generator [11].

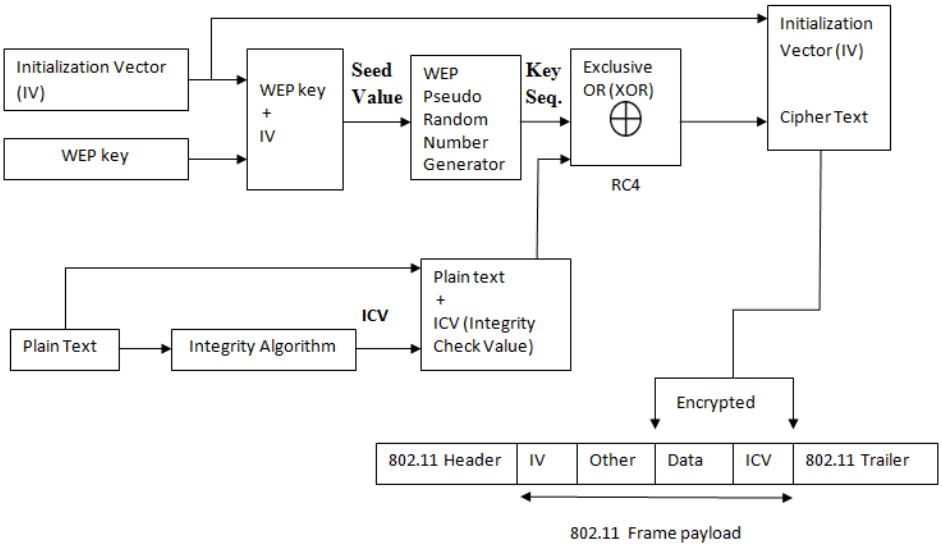

Figure 3: WEP Encryption Process [12, 13]

iii. Integrity Algorithm CRC-32 is performed on plain text to generate Integrity Check Value (ICV) which is concatenated with plain text.

iv. RC4 algorithm is applied on Plain text + ICV and Key sequence to generate cipher text.

v. The payload for the wireless MAC frame is created by adding the IV to front of the encrypted combination of data and ICV along with other fields.

II. WEP Decryption Process consists of following steps:

i. Initialization vector from 802.11 frame payload is concatenated with WEP key. This acts as seed value for Pseudo Random Number Generator.
ii. CR4 algorithm is applied to cipher text of frame payload and key sequence to get plain text.
iii. Plain text and original ICV are obtained.
iv. Plain text is input to Integrity algorithm to generate new ICV.
v. New ICV is compared with original ICV to get the result.

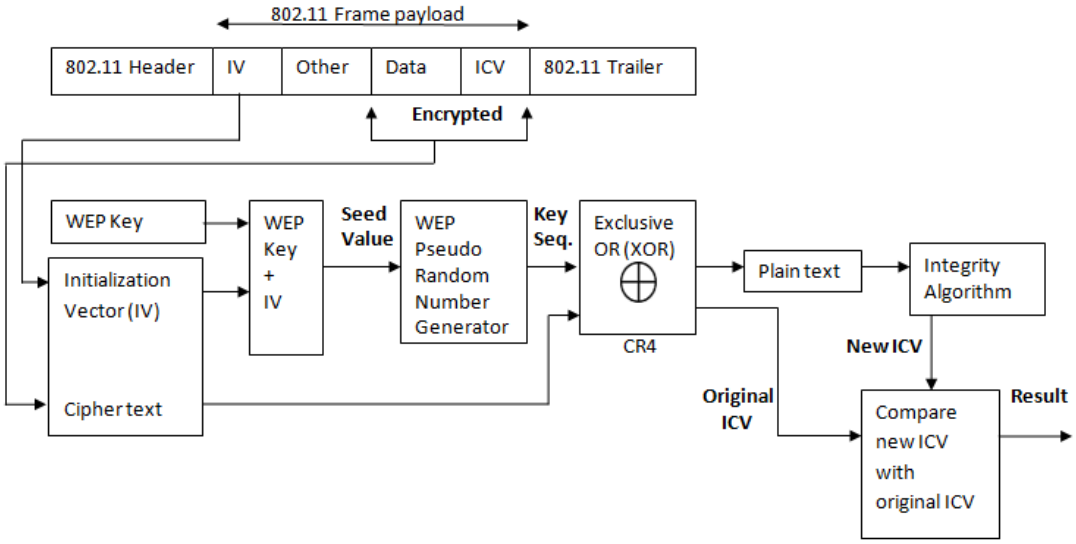

Figure 4: WEP Decryption Process

III. WEP Shortcomings

1) Weak Cryptography: Analysis of captured traffic can easily reveal the shared key used by WEP. Various tools are available which enable data decryption within few minutes [14, 15].
2) Absence of Key Management: WEP does not provide key management and thus, same keys are used for longer duration and tend to be of poor quality [16].
3) Small key size: The standard specified for WEP provides support for 40 bit key only, thus it is prone to brute force attacks. Offline dictionary attack is a type of brute force attack where frequently used words for encryption are considered and the result is compared with captured traffic to reveal the secret pass phrase.
4) Reuse initialization vector: Initialization vector is reused and thus, data can easily be decrypted without the knowledge of encryption key using various cryptanalytic methods.
5) Lack of Replay protection: WEP does not provide protection against replay attacks, thus, an attacker can record and replay packets and they will be accepted as genuine.
6) Authentication issues: Challenge-response scheme is used in shared key authentication but it can lead to man-in-the-middle attack. Man-in-the-middle attacks set up illegitimate access points within range of wireless clients in order to gain access to sensitive information.
7) Jamming: Availability can be impacted i.e. electromagnetic energy emitted on wireless LAN's frequency by a device making WLAN unusable.
8) Packet Forgery: WEP does not provide any protection measures against packet forgery.
9) Flooding: An attacker can send large number of messages to access point (AP) and thus, preventing the AP from processing the traffic [17].

B. Wi-Fi Protected Access (WPA):

The WPA protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP. WPA uses the Temporal Key Integration Protocol (TKIP) algorithm for encryption. TKIP is a security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and a solution was required for already deployed hardware [18].

WPA has following advantages:

- A cryptographic Message Integrity Code (MIC), called Michael, 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 alterations. 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 the 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 was based on the Pair Wise Master key (PMK) that is derived from the concatenation of the passphrase, Service Set Identifier(SSID), length of the SSID and nonces (a number or bit string used only once in each session).
- 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 decrypt the encrypted message with each generated permutation, and validate the output by means of cross comparison with words, file header and any other data.
- Placement of MIC: It is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack.

C. Wi-Fi Protected Access2 (WPA2)

WPA2 protocol uses the more robust encryption algorithm known as Advance Encryption Standard (AES). Advanced Encryption Standard is a symmetric-key encryption standard adopted by the U.S. government. AES was announced by National Institute of Standards and Technology (NIST) [19]

After a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable. The Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. There are various advantages of WPA2.

Advantages of WPA2 include:

- WPA2 supports IEEE 802.1X/EAP (Extensible Authentication Protocol) authentication or Pre Shared Key (PSK) technology. A pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. Such systems almost always use symmetric key cryptographic algorithms. Thus removing the passphrase choice problem of WPA.
- It also includes a new advanced encryption mechanism using the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) called the Advanced Encryption Standard (AES). Thus providing security against most of the attacks encountered due to weak encryption key.

Although WPA2 uses more robust security algorithm i.e., AES but it also has some problems like:

- 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 decrypt the encrypted message with each generated permutation, and validate the output by means of cross comparison with words, file header and any other data.
- Placement of Message Integrity Check (MIC) bits: It is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack.

Time Factor: It is a very important factor in which we measure how long will it take to brute force a protocol, currently this is done by calculating how many permutations are there in the encryption/ decryption key. As the processing power of the computers is ever increasing WPA2 protocol requires small time to brute force [20].

5. Conclusion

Wi-Fi security is not an easy task. Wireless network security is more difficult than wired network security. There are many protocols or standards or we can say technologies for wireless network security but every protocol has its demerits, until now there is no protocol which can provide security 100% or near about it. Many researchers are working on it and they are searching for the best protocol which can provide security as much as possible.

In this paper, we show the WiFi security by reviewing the related standards WEP, WPA and WPA2 and were presented the operation of WEP, and described its advantages and weaknesses. We also described the some of security attacks.

We conclude that WEP encryption does not provide sufficient wireless network security and can only be used with higher-level encryption solutions (such as VPNs). WPA is a secure solution for upgradable equipment not supporting WPA2, but WPA2 will soon be the standard for wireless security.

References

[1] Introduction to WI-FI network security by Bradley Mitchell, About.com.
[2] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.
[3] Wireless network security 802.11, Bluetooth and handheld devices by Tom Karygiannis, Les Owens.
[4] WEP, WPA, WPA2 and home security by Jared Howe.
[5] http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php
[6] The state of WI-FI security by WI-FI Alliance.
[7] Establishing wireless robust security networks: a guide to IEEE 802.11i by Sheila Frankel Bernard Eydt Les Owens Karen Scarfone.
[8] http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

[9] S. D. Kanawat and P. S. Parihar, Editors, "Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, (2011) May 18-23.
[10] Jason Bonde, Wireless Security, University of Minnesota UMM CSci Senior Seminar Conference Morris, MN.
[11] K. Benton, ―The evolution of 802.11 wireless security‖, INF 795, April 18th, 2010. UNLV Informatics-Spring 2010.
[12] Arash Habibi Lashkari, Masood Mansoori, Amir Seyed Danesh, ―Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)‖, in ICCDA Singapore Conference, 2009
[13] Microsoft Technet Library, How 802.11 Wireless Works, Technical Reference, Available: http://technet.microsoft.com/en us/library/cc757419(WS.10).aspx
[14] Scott Fluhrer, Itsik Mantin, Adi Shamir, ―Weaknesses in the Key Scheduling Algorithm of RC4‖, In Eight Annual Workshop on Selected Areas in Cryptography, August 2001.
[15] 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
[16] Halil Ibrahim Bulbul, Ihsan Batmaz, Mesut Ozel, ―Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols‖; in Proceedings of the 1st international conference on Forensic applications and techniques, information, and multimedia and workshop, (Adelaide, Australia, January 21-23, 2008), ICST, Brussels, Belgium, 2008
[17] Arockiam .L. and Vani .B, ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network‖, International Journal on Computer Science and Engineering, Vol.02, No. 05, pp. 1563-1571, 2010.
[18] Y. X. Lim and T. Schmoyer, Editors, "Wireless Intrusion detection and response", IEEE Information Assurance Workshop, (2003) June 18-20, Westpoint, Newyork.
[19] Stamatios and V. Kartalopoulos, Editors, "Differentiating Data security and Network Security", IEEE International Conference on Communications, (2008) May 19-23, Beijing.
[20] K. Bhatele, A. Sinhal and M. Pathak, Editors, "A Novel Approach to the Design of New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram.