# SECURITY OVER WI-FI

Dr. Sunil Kumar Vats

*PGT (Computer Science), Jawahar Navodaya Vidyalaya, Kotia, Mohindergarh, Haryana, India*

***Email ID**: sunilvats1981@gmail.com*

**Received**: 09.01.2017 **Accepted**: 19.02.2017

**Keywords**: WI-FI, WEP, SSID, MAC, WiMAX, DoS, IEEE, Wireless Security.

## Abstract

*Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. Wireless technology has many benefits over wire based technology in terms of portability, flexibility, productivity, and installation costs. Wi-Fi networks can be accessed by using any electronic gadget (Mobile, Laptop etc). Wireless technologies have gaining their platform rapidly 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. Since the IEEE ratification of the 802.11 standard in 1997, this paper describes the justification for a project to assess the security status of wireless network usage in society. It also reviews the commercial and residential approaches to wireless network security status in the county. By War Driving these conurbations, actual data was gathered to indicate the security status of wireless networks and give a representation of modern attitudes towards wireless security for the sample population. Preliminary results are presented to demonstrate the extent to which commercial or residential conurbations address wireless security. At this stage in the research further work is required to completely analyse the results. It is anticipated that the results will be useful for providing input into a defence and attack methodology for improving the security of both residential and commercial use of wireless networks.*

## Paper Identification

## 1. Introduction

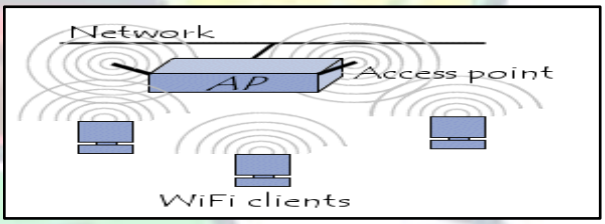
Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi alliance, the organization that owns the wi-fi term specifically defines Wi-Fi as any ―wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers (IEEE). A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked phrase that

means IEEE 802.11x. 802.11 standards." 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. 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. 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 bandwidth. In Latest trends United State is the top country using the services of wi-fi in the world. India is even out of the list of top 10 countries, who are using Wi-Fi Services.

## 2. IEEE 802.11

IEEE 802.11 is a basic standard for Wireless Local Area Network (WLAN) communication. IEEE 802.11 standard was first introduced in 1997. It was envisioned for home and office environments for wireless local area connectivity and supports three types of transmission technologies namely *Infrared (IR),Frequency Hopping Spread Spectrum (FHSS),Direct Sequence Spread Spectrum (DSSS).* In 1999 two other transmission technologies were included Orthogonal Frequency Division Multiplexing (OFDM) and High Rate Direct Sequence Spread Spectrum (HR-DSSS). The second OFDM modulation scheme was introduced in 2001 for high data rates. The standard introduces two operating modes of wireless networks, namely, the infrastructure networks and the ad hoc networks. The infrastructure operating mode (Figure) is a network with an Access Point (AP), in which all STAs must be associated with an AP to access the network.




STAs communicate with each other through the AP. An infrastructure one with planned, permanent network device installations. It can be set up with a fixed topology, to which a wireless host can connect via a fixed point, known as a base station or an access point. The latter is connected to the backbone network, often via a wired link. Cellular networks and most of the wireless local area networks (WLANs) operate as the static infra-structured networks. All wireless hosts within the transmission coverage of the base station

can connect to its signal and use it to communicate with the backbone network. This means that all communications initiated from or destined to a wireless host have to pass through the base station to which the host connects directly. In addition, an infra-structured network is also be established with a quasi-static or a dynamic topology. A satellite network belongs to this category. It has a space segment and a ground segment. The space segment comprises of satellites. The ground segment has a number of base stations, also known as gateway stations (GSs), through which all communications via long-haul satellite links take place. The base station, or access point, is a critical element for communication.

## 3. Wireless Networks Challenges

Wireless Networks plays the most important role in the development of the information in between individual to individual, business to business, and individual to business. It changed completely the way of sharing of the information but still there are lot of challenges which are the hurdles in the wide adaptation of wireless network technology. We have to understand the main problems that not only WI-FI network faces but all the networks faces are –CIA that is **C**onfidentiality, **I**ntegrity and **A**uthentication.

**Confidentiality**: Allow only the authorised person to read the encrypted messages or the information.

**Integrity**: It is defined as the information not being opened by third person and it should reach in the same format as it was sent by the sending party.

**Authentication**: The parties sending or receiving messages make sure that, who they say they are, and have right to undertake such actions.

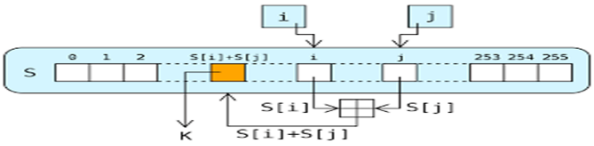
The main issue in the security of wireless signal is its mode of transmission .wireless signals are transmitted through the electromagnetic waves; these waves cannot be contained physically. In wireless networks the signals are communicated via air, hence can be easily intercepted with the help of right transceiver equipment.

## 4. 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. 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-compliantproducts are backward compatible with IEEE 802.11b-compliant products.

**WEP**

WEP (Wireless Equivalent Privacy) protocol is part of the IEEE 802.11 standard. It was ratified in 1997 with the intension to provide data confidentiality comparable to that of a traditional wired network. WEP was the first cryptographic protocol which are developed for the WI-FI to enable privacy and authentication .WEP uses the shared key authentication mechanism and is based on secret cryptographic key.

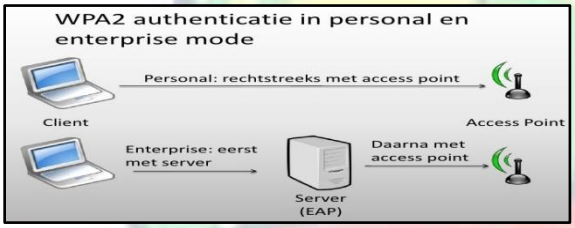



WEP protocol uses the RC4 (Rivest Cipher4 also known as ARCFOUR meaning Alleged RC4) stream cipher algorithm to encrypt the wireless communications. This RC4 (Figure) stream algorithm

protects the contents form disclosure to eavesdroppers. WEP support 40-bit key and with extension it also support 128 or even 256 bit key also .WEP was designed to protect a wireless network from eaves dropping. WEP uses linear hash function for data integrity. In WEP there is no key management and no replay detection facility. But in 2001 several serious weaknesses were identified. Now, WEP connection can be cracked within minutes. After having such type of vulnerabilities, in 2003 the WI-FI Alliance WEP had been replaced by WPA .The main problem of WEP was-it uses static encryption keys.

**WPA/WPA2**

WPA (Wi-Fi Protected Access) WPA2 are two security protocols developed by WI-FI Alliance. WPA provides developed with the purpose of solving the problems in WEP cryptographic method. WPA was developed in 2003. Both WPA and WPA2 have two modes of operation:




**Personal and Enterprise**

This mode involves the use of a pre-shared key for authentication, on the other hand Enterprise mode uses IEEE 802.1X and EAP. Wi-Fi Protected Access II was introduced in September 2004 with a subset of the IEEE 802.11i specification that addresses the weaknesses of WEP. WPA2 extends WPA to include the full set of IEEE 802.11i requirements. It is easier to configure and is more secure than Wi-Fi Protected Access. WPA uses the improved encryption algorithm known as Temporal Key Integrated Protocol (TKIP).TKIP provides each client with a unique key and uses much longer keys that are rotated at a configurable interval. It also includes an encrypted message integrity check field in the packets; this is designed to prevent an attacker from capturing, altering and/or resending data packets which prevent DoS and spoofing attack. WPA can be operated with or without of RADIUS severs. Wi-Fi Protected Access II uses Advanced Encryption Standard. Older Network card stop in its smooth working. Wi-Fi protected Access have four key factors:

- Mutual Authentication
- Strong Encryption
- Interoperability
- Ease to use

The fundamental aspect of Wireless Networks in maintaining security is to maintain Confidentiality where the receiver should receive the actual transmitted information from the sender. The message authentication provides integrity to both sender as well as receiver. The Wireless Link should be always available and should be secured from outside world like malicious attacks as well as DoS Attacks (Denial of Service Attacks).

There are basically two common attacks which compromise the security and authentication mechanism of Wireless Networks i.e. Message Reply Attack and Man in the Middle Attack. The Message reply attack acts principally on the authentication and authentication key formation protocols. The Man in the Middle Attack (MiTM) attack occurs on that security mechanism which doesn't provide mutual authentication.

Various other attacks like Session Hijacking, Reflection attacks are there which affects the security mechanism of Wireless Networks.

IEEE helped in securing the wireless networks by providing the basic measures for securing wireless network and it also provide CIA factors by disabling SSID, use of MAC i.e. Media Access Control address filtering and WPA/WPS protection mechanism. The

recent developments in computer technology and software developments notice that these mechanisms have network vulnerable attack. So, due to these vulnerabilities WiMax standards comes into existence, for solving the short comings of 802.11 wireless networks. WiMax is the new advancement in the wireless network. WiMax is still undergoing development and still the securing problems are not being decreased by WiMax technology. It also has some drawbacks like it lack mutual authentication and is suspected to relays attacks, spoofing of MAC address of Subscriber Station (SS) and PMK authorization vulnerabilities.

## 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. WiMaX is the recent technology in the Wi-Fi security. It also has some deficiencies.

## RÉFÉRENCIAS


[1] Wireless security: an overview by Robert J.Boncella. Washburn University ZZbonc@washburn.bdu.

[2] White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications.

[3] Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.

[4] Security Issues on Converged Wi-Fi & WiMAX Networks by Prof. Anand Nayyar, Lecturer, P.G. Department of Computer Science, K. L. S. D College Ludhiana ,anand_nayyar@yahoo.co.in .

[5] Wireless network security? Author:-Paul Asadoorian, GCIA, GCIH. Contributions by Larry Pesce, GCIA , GAWN PaulDotCom.

[6] Securing Wi-Fi network (10 steps of diy security) by Rakesh M Goyal and Ankur Goyal

[7] Establishing wireless robust security networks: a guide to IEEE 802.11i by Sheila Frankel Bernard Eydt Les Owens Karen Scarfone.

[8] Wireless LAN security today and tomorrow By Sangram Gayal And Dr. S. A. Vetha Manickam.

[9] Introduction to WI-FI network security by Bradley Mitchell, About.com.

[10] The state of WI-FI security by WI-FI Alliance.

[11] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.

[12] Wireless network security 802.11, Bluetooth and handheld devices by Tom Karygiannis, Les Owens.

[13] WEP, WPA, WPA2 and home security by Jared Howe.