ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 09, pp.57518-57520, September, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

WI-FI:THE MODERN TRENDS OF TECHNOLOGY

***Sandip Kumar Pan**

Jharkhand Rai University, Ranchi, India

ARTICLE INFO

Article History:
Received 14th June, 2017
Received in revised form
20th July, 2017
Accepted 03rd August, 2017
Published online 29th September, 2017

Key words:

Wireless Fidelity Technology,
Wired Equivalent Privacy (WEP),
Wireless Fidelity Protected Access (WPA),
Wireless Access Point,
SSID, MAC, WiMAX, DoS

ABSTRACT

Wireless networks are very popular nowadays. Wi-Fi® is a system of wirelessly connecting devices that use radio waves, allowing for connection between devices without the expense of cumbersome cables or without needing them to be facing one another. Wi-Fi stands for Wireless Fidelity® and is used to define the wireless technology in the IEEE802.11b standard. It operates in the unlicensed 2.4 GHz radio spectrum, uses direct-sequence spread spectrum (DSSS) for modulation, supports variable data rates up to 11 Mbps, and has a range of about 50 meters. Wireless technology provides us much profit like portability and flexibility, increased productivity, and lower installation costs. Nowadays, communications through mobiles, computers, laptops, wireless networking technologies have extended to a great level. This does a maximum coverage all over the world. Security issues have also been crossed a level in Wi-Fi network because of the unauthorized users and the Wi-Fi hackers. So to implement the feasible Security WEP, WPA has been proposed in this paper to overcome the feasible security problems. These both protocols are generally used to encrypt the current data and information, so that the unauthorized and hackers cannot be able to decrypt the data and hack the Wireless Fidelity (Wi-Fi) networks. Many accessories can be connected with the Wireless Fidelity network with the help the Access Point (AP).

Citation: Sandip Kumar Pan, 2017. "WI-FI:The modern trends of technology", *International Journal of Current Research*, 9, (09), 57518-57520.

INTRODUCTION

Wireless Fidelity Wi-Fi Technology is one of the upcoming techniques in the internet world. This Wi-Fi can be an alternate to Wired Technology. Wi-Fi is usually used for linking devices in wireless form. Wi-Fi Network attaches computers to one another in a better communicable way. It creates a hidden path between the internet and the wired network. Wi-Fi network functioning can be done on the physical and the data link layer. Radio Frequency (RF) is used for transmitting data through air. This is the very characteristic in the Wi-Fi technology. It also provides enhanced data speeds. IEEE 802.11 is considered as a position of values moving elsewhere can be known as Wireless Local Area Network (WLAN). This is also a type of network communication. Access Point (AP) is considered as very significant feature in the Wi-Fi network technology. Access Point (AP) has a radio transmitter and also a radio receiver. This directly gets linked with the wired network or to the internet network.

Research article open AC

This Access Point (AP) takes a common achievement as a base station for the entire Wi-Fi net-work. Some of the Wi-Fi Network Topologies are given below.

Corresponding author:* **Sandip Kumar Pan,
Jharkhand Rai University, Ranchi, India

-> Access Point AP-based topology
-> Star-based network topology
-> Peer-to-peer topology
-> Point-to-multipoint bridge topology

Fig.1. Wi-Fi Technology

Fig. 2. Wireless Access Point

This Wi-Fi network is facing numerous security problems because of the hackers and also by the unauthorized members. The Wi-Fi hacker uses the Wireless Hacking tools AirSnort, Aircrack, WepAttack, WEPCrack etc above the network. Wireless Access Point is shown in the Figure 2. It basically helps to connect with devices likes digital cameras, tablet computers and digital audio players, PCs, video-game comforts, smart phones, laptops etc.

Related work

Wireless is in everywhere like

- More devices are using Wi-Fi:- Cell phones
- Digital cameras
- Printers
- PDAs
- Video game controllers
- Televisions
- Speakers
- Refrigerators etc

Wireless networks challenges

Wireless Networks plays the most significant role in the development of the information in among individual-to-individual, business-to-business, and individual-to-business. It changed entirely the way of sharing of the information but still there are lots of challenges which are the hurdles in the wide adaptation of wireless network technology (Robert J.Boncella, 2002) White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications, 2009). We have to understand the main harms that not only WI-FI network faces but all the networks faces are –CIA that is confidentiality, integrity and authentication.

Confidentiality

Allow only the authorized person to examine 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 transfer party.

Authentication

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

802.11 – applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHzband using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

802.11a – an extension to 802.11 that applies to and provides up to 54 Mbps in the 5GHzband. 802.11a uses an orthogonal frequency division multiplexing encoding scheme ratherthan FHSS or DSSS.

802.11b (also referred to as *802.11 High Rate* or Wi-Fi) – an extension to 802.11 that applies to wireless and provides 11 Mbps transmission (with a fallback to 5.5, 2.0, and 1.0 Mbps) in the 2.4 GHz band. The 802.11b uses only DSSS. It has been the 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to the Ethernet.

802.11g – applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

There are many wireless LAN technologies nowadays, such as, Wi-Fi, Bluetooth, HiperLAN, HomeRF, etc. All these technologies operate in the 2.4-GHz ISM (Industrial, Scientific, and Medical)radio spectrum. Each technology has its own niche depending on the deployment requirements of the wireless LANs. The only technology, which has received the widest market acceptance, is IEEE 802.11bor Wi-Fi. The popularity of this standard is aptly reflected in portable computer vendors' decision to integrate 802.11b wireless network adapters with notebook computers.

WEP

WEP protocol is element of the IEEE 802.11 standard (Dr. Andy Ju An Wang Spring, 2004), (Sangram Gayal and Vetha Manickam, 2002), (Bradley Mitchell, 2015), (The state of WI-FI security by WI-FI Alliance), (WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre), (WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre). It was introduced in 1997.WEP is used in 802.11 network to defend link level data during the wireless transmission. WEP was the first cryptographic protocol which are developed for the WI-FI to facilitate privacy and authentication. WEP uses the shared key authentication mechanism and is based on secret cryptographic key. WEP protocol uses the RC4 (Rivest Cipher 4) stream cipher algorithm to encrypt the wireless communications. This RC4 stream algorithm protects the contents form disclosure to eavesdroppers. WEP support 40-bit key and with addition 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 trouble of WEP was-it uses static encryption keys.

WPA/WPA2

WPA and WPA2 are two security protocols developed by WI-FI Alliance (Introduction to WI-FI network security by Bradley Mitchell, About.com), (The state of WI-FI security by WI-FI Alliance), (The state of WI-FI security by WI-FI Alliance), (The state of WI-FI security by WI-FI Alliance). WPA provides developed with the point 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. The Personal mode involves the use of a pre-shared key for authentication, while the Enterprise mode uses IEEE 802.1X and EAP for this point.WPA2 was introduced in September 2004. WPA addresses 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. WPA is easier to configure and it is extra secure

than WEP. WPA uses the improved encryption algorithm known as TKIP (Temporal Key Integrated Protocol).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 avoid an attacker from capturing, altering and/or resending data packets which prevent Denial-of-Service and spoofing attack. WPA can be operated with the help of RADIUS server of without RADIUS severs. Now, TKIP can be broken easily. WPA2 uses Advanced Encryption Standard. WPA2 may not work with some older network cards. WPA2 have the 4 main key factors:-

- Mutual authentication
- Strong encryption
- Interoperability
- Ease to use

Recent LiFi over WiFi

The new technology Light Fi (LiFi) is LED switching on/of technique which transfers data at high speed. The speed of the on and of switching of the LED is converted in terms of data rates. The speed is 1Gbits/sec. which is 10 times faster than WiFi

Conclusion

Wi-Fi security is not an simple task. Wireless network security is harder than wired network security. There are numerous 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 various deficiencies.

REFRENCES

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

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

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

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

Security Issues on Converged Wi-Fi & WiMAX Networks by Prof. Anand Nayyar, Lecturer, P.G.

The state of WI-FI security by WI-FI Alliance.

WEP, WPA, WPA2 and home security by Jared Howe

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

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

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

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

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

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

****