A Latest Review of 4G and 5G Mobile Wireless Networks Techniques in Wi-Fi Networks Architecture and Challenges

[1] **Umesh Seghal,** [2] **Vimal Dev**

[1,2] GNA University FCS
Phagwara , Punjab 144401, India

Abstract - Wireless technologies have become increasingly popular every day in business as well as in personal lives. Wireless technology provides us many benefits like portability and flexibility, increased productivity, and lower installation costs. The IEEE 802.11 specification (ISO/IEC 8802-11) is an international standard describing the characteristics of a wireless local area network (WLAN). The name Wi-Fi (short for "Wireless Fidelity", sometimes incorrectly shortened to Wi-Fi) corresponds to the name of the certification given by the Wi-Fi Alliance, formerly WECA (Wireless Ethernet Compatibility Alliance), the group which ensures compatibility between hardware devices that use the 802.11 standard. Today, due to misuse of the terms (and for marketing purposes), the name of the standard is often confused with the name of the certification. In this paper we are discussing about the wireless network challenges and IEEE 802.11 Standards and WEP protocol. Currently the 4G's concept is marching towards the standardization phase. So time has come to introduce a new technology in which we can connect to multiple wireless technologies, networks, terminals and applications, all simultaneously and can also switch between them. This latest technology is named as 5G.

Keywords - *WI-FI, WEP, SSID, MAC, Wi MAX, DoS*

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." Mobile is a radio terminal that can be moved during operation or it may be attached to a fast moving vehicle or portable hand set. We can say a mobile is a radio, because it also radiates electromagnetic waves or radio waves just like a radio. In the process of communication, man has seen a number of changes. The technology creation, revolution and evolution of the wireless mobile had started since the early of 1970s. In the modern world of communication system, cellular telephone began as a simple concept. The increased demand for cellular services has caused cellular telephone systems to evolve in to complicated networks and internet comprised of several types of cellular communication systems. The cellular concept is used in some full-duplex systems like standard cellular telephone services (CTS), personal communications systems (PCS), and personal communication satellite system (PCSS).

Technologies like frequency modulation (FM) and frequency shift keying (FSK) were used previously in cellular communication system. FM was used for voice and FSK was used for transporting controlling and signaling information. Now days some advanced digital communication techniques like Quadrature phase shift keying (QPSK), Minimum shift keying (MSK) are used in wireless cellular communication system and also some new frequency bands has been assigned by Federal Communication Commission (FCC). Presently, the use of landline has come to an end. We are now actually living in the era of convergence. The word convergence denotes merging of technologies, domain and discrete IT systems. The basic part of convergence is digitization which is accomplished through Analog-to-Digital Converters (ADC).

2. Related Work

Wireless is in everywhere like-More devices are using Wi-Fi:- Cell phones, Digital cameras, Printers ,Scanners

,PDAs, Video game controllers, Televisions, Speakers, etc. [5].

3. Wireless Networks Challenges

After a brief introduction to 5th generation wireless systems, this section briefly outlines the evolution of mobile communication technology from 1G to 5G.In [3], the authors have described that, the First generation cellular system (1G) were analog telecommunications standards introduced in the 1970s. Here the voice channel used frequency modulation, and they used frequency division multiple access (FDMA) techniques. The major disadvantages of 1st generation wireless systems are poor voice quality, poor battery quality and large phone size. 2G was introduced in 1980s.[9] The 2G systems were digital and were oriented to voice with low speed data services. 2G used GSM technology and GSM stands for global system for mobile communication. It is a circuit switched, connection based technology, where the end systems are devoted for the entire call period. Therefore, it causes low efficiency in usage of bandwidth and resources. Generally GSM enabled systems don't support high data rates and they are generally unable to handle complex data like video. Next comes 2.5G. 2.5G is not an officially defined term rather it was invented for marketing purpose.

3G stands for 3rd generation wireless system. It has the capability to handle complex data like video and also it supports high data rates. Generally 3G wireless systems use Code Division Multiple Access Technique (CDMA). The 3G technology adds multimedia facilities to 2G phones by allowing video, audio, and graphics applications. Apart from that, 3G promises increased bandwidth, 384 kbps when the device holder is walking, 128 kbps in a car and 2 Mbps in a fixed application. 4G stands for 4th generation wireless system. It has been lunched in many countries. In 2009 IMT-A specified the requirements for 4G standards. A 4G system is expected to provide a comprehensive and secure based solution to laptop and mobile devices. Such as internet access, gaming services and streamed multimedia may be provided to users. The technologies like Coded Orthogonal Frequency Division Multiplexing (COFDM), Multiple Input Multiple Output (MIMO) and link adaptation are used in 4th generation wireless system.

3.1 Confidentiality

Allow only the authorized 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.

3.2 WEP

The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

3.3 WPA/WPA2

Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. [4] [12,14]Most current WPA implementations use a presoaked key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates. Based on the 802.11i wireless security standard, which was finalized in 2004? The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret — it's probably good enough to protect your secrets as well.WPA2 have the 4 main key factors:-

1. Mutual authentication
2. Strong encryption
3. Interoperability
4. Ease to use.

These are the 4 main advantages of WPA2. WPA and WPA2 use the cryptographic hash function for data integrity. WPA and WPA2 both provides the key management and replay detection. 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 [4]. 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. we can summarize the applications.

1. One can be able to feel her kid's stroke when he/she is in her mother's womb.
2. One can be able to perceive his/her sugar level with his/her mobile.
3. One can be able to charge his/her mobile with his/her own heartbeat.
4. One can be able to view his/her residence in his/her mobile when someone enters.
5. The mobile will ring according to our mood.
6. One can be able to pay all bills in a single payment with his/her mobile.
7. One can get the live share value.

4. Conclusions

Wi-Fi security is not an easy task. Wireless network security is more difficult than wired network security. The future is becoming more and more difficult to predict with each passing year. So we should always expect an increasing pace of technological change. In this paper, the main importance is on 5G mobile phone concept and its architecture which is going to be a new mobile revolution in mobile market. The 5G technologies incorporate all type of advanced features which makes 5G mobile technology most powerful and in huge demand in near future. 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. Worldwide Interoperability for Microwave Access – should be capable of around 40 megabits per second with a range of 30 miles. It is one of the closest technologies to meet the standards of true 4G and as it develop should surpass the 100MB/second which is the 4G standard. Mobile WiMAX allows the use of high speed data transfers and is the main competition for the 4G LTE services provided by cellular carriers. The major wireless networks are not actually lying to anyone about 4G, they simply stretch the truth a bit. A 4G phone has to comply with the standards but finding the network resources to fulfill the true standard is difficult. You are buying 4G capable devices but the network is not yet capable of delivering true 4G to the device. Your brain knows that 4G is faster than 3G so you pay the price for the extra speed.

References

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

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

[3] Paul Asadoorian, " Wireless network security ", GCIA, GCIH. Contributions by Larry Pesce, GCIA , GAWN PaulDotCom.

[4] Paul Asadoorian, " Wireless network security? ", GCIA, GCIH, GAWN PaulDotCom.

[5] Rakesh M Goyal and Ankur Goyal, " Securing Wi-Fi network (10 steps of diy security) ".

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

[7] Sangram Gayal And Dr. S. A. Vetha Manickam, " Wireless LAN security today and tomorrow ".

[8] Sangram Gayal And Dr. S. A. Vetha Manickam, " Wireless LAN security ".

[9]http://compnetworking.about.com/od/wirelesssecurity/a/introduction-to-wifi-network-security.htm

[10]http://www.hsc.fr/ressources/articles/hakin9_wifi/index.html.enWireless network security 802.11, Bluetooth and handheld devices by Tom Karygiannis, Les Owens.

[11] A. A. Name, "Conference Paper Title", in Conference Name, Year, Vol. x, pp. xxx-xxx.

[12] http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html.

Umesh Sehgal, Assistant Professor in GNA University, Phagwara.He has completed M.Phil, MCA, M.Sc (CS).He had 14 years of Teaching Experience.

Vimal Dev, Assistant Professor in GNA University, Phagwara.He has completed M.Tech, B.Tech. He had 01year of teaching experience.