Survey on Wireless Network Security Threats and Security Measures

[1]Ibrahim Mohamed Hussain Adam
[1]Research Scholar
[1]Rathinam College of Arts and Science

***Abstract* - Nowadays computers and smart electronic devices are in everywhere in all over the world that is why wireless network has become very popular and available in everywhere like airports, banks, organizations, college, schools, companies, restaurants, cafes, houses and etc. Wireless network can be access through electronic devices which has network sensor that allows them to join the wireless LAN. Internet security (Network security) also is a big topic that is very important in our society communication system and for it is extremely dynamic and wide in scope. This is the reason that many companies and organizations invest heavily in a dedicated infrastructure security and highly trained specialists. The aim of security monitoring and preventing the network from cyber threats requires vigilance over the network equipment. [1] Wireless network plays a great role in order to facilitate our daily life and make everything depend on the internet very easy, it totally changed our way of exchanging information and communication by decrease the location and distance. In this paper we are attempt to analyze wireless network 802.11 standard and WEP protocols. Beside the general security goals like confidentiality, integrity, availability [2]**

***keywords* - Wireless Network; Wireless Network Security; Wireless LAN**

I. INTRODUCTION

Wi-Fi is stand for wireless fidelity is generic term that refers to IEEE 802.11 which use radio waves to provide wireless high speed internet and network connection. Rapid development in wireless network has considerable growth in recent years. Wireless network include several nodes which communicate with each other on more than a wireless channel, because it work with no physical wired connection between sender and receiver by using Radio Frequency (RF) technology only. And when RF supplied current to an antenna, an electromagnetic field is related, and then is able to propagate through space. Although the elements of any wireless network is an **Access point** (AP) the AP is a wireless LAN transceiver or (base station) that can connect one or many wireless devices simultaneously to the internet. **Wi-Fi Card** they accept the wireless signal and relay information they can be internal and external. Computers and smart electronic devices must have Wi-Fi card or wireless network adapter in order to receive the signal and join the wireless network. **Safeguard** firewalls and anti-virus software protect networks from uninvited users and keep the Wi-Fi network and information secures.

II. RELATED WORK

The IEEE 802.11-based network also called WI-FI networks are expanding into mainstream areas of Business from their traditional applications in warehouses for the retails floors. As a result, it is important to have the necessary tools to troubleshoot and protect networks. Network security has come a long way since the early days and the negative around the shortcomings of WEP.[3] also in order to understand the potential threats to an ad hoc network, it is important to consider the nature of such networks. The term ad hoc is Latin and it literally means "for this "as in "for this specific purpose." As the name suggests, ad hoc networks are typically designed for a specific purposes and to work autonomously without having to rely on existing infrastructure. [4] Wireless mesh network enclose mesh router and mesh customer that constitution multi-hop wireless network. Present are two approaches used in mesh network for protocol intend. The protocols are design with full simplicity and independency of layer from each additional. In conjectural framework, the difficulty is decompose according to the occupation of primal or language dual erratic.[5] Due to the significance attached to the applications of MANET, security in ad hoc networks is a hot research area and already considerable research is done in this field. Use of wireless links renders an ad-hoc network susceptible to link attacks ranging from passing eavesdropping to active impersonation, message replay and message distortion. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. [6]

III. NETWORKING

A wireless network enables people to communicate and access applications and information without wires. This provides freedom of movement and the ability to extend applications to different parts of a building, city or anywhere in the world. Wireless networks allow people to interact with e-mail or browse the internet from a location that they prefer. Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computer devices. These devices include personal digital assistants (PDAs), laptops, personal computers (PCs), servers, and printers. Computer devices have processors, memory, and a means of interfacing with a particular type of network, traditional cell phones don't fall within the definition of a computer device, and however, newer phones and even audio headsets are beginning to incorporate computing power and network adapters. Eventually most electronics will offer wireless network connection.

As with networks based on wire, or optical fiber, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, and database records, streaming video or voice. In most cases, wireless networks transfer data, such as e-mail messages and files, but advancements I the performance of wireless networks is enabling support for video and voice communications as well.

IV. TYPES OF WIRELESS NETWORK

Wireless PAN: Wireless PAN Stands for wireless personal area network. Wireless PAN is used for transmission of data over the shorter distance like the data transfer between two devices. The two example of Wireless PAN is Bluetooth and Infrared. A Bluetooth device uses WPAN technology. This is used to transfer the data over the shorter distance. The operation of Bluetooth device works only on MAC layer and physical layer whereas Infrared is used to transfer the data in linear order. Wireless PAN is the network that does not require any fixed infrastructure and data transfer are cheaper in Wireless PAN.

Wireless LAN: Wireless LAN stands for wireless local area network. It is used for small area like school, office. It has the radius of 100-300 feet. These networks allow the connection in the local area like school, office, and library. Wireless LANs support a cellular architecture. The organization is subdivided into cells and is managed by Base station. Wireless LANs use radio or infrared light to provide internet signal. These provide a mobile access, and provide a better throughput compared to the wired Ethernet.

Wireless MAN: Group of network that provides wireless connectivity to a metropolitan city is known as wireless metropolitan area network. The goal of WMAN is to extend the area covered by LAN network in manner that network should be cost efficient, and support high speed, without extending the wired connection in a network. The WMAN provide mobility to the node with high speed internet in the metropolitan area.

Wireless WAN: Homes and small offices enhanced the growth of WLANs after new wireless networking standard IEEE 802.11n came in existence in 2009. All laptops, tablets and smart phones are equipped with WLANs component and some coffee shops, hotels and public places like shopping malls are also facilitated with WLANs. Wireless Network Interface Cards (NICs) and Access Points (APs) are required along with Internet Service Provider and a device for communication to occur. Low speed WLANS offers of about 1 and 2 Mbps whereas higher data rates WLANs offers up to 1 Gbps and above. IEEE 802.11a offers maximum speed of 54 Mbps and transmission at 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12Mbps, 9 Mbps and 6 Mbps are also supported thus allowing faster data transmission rate.

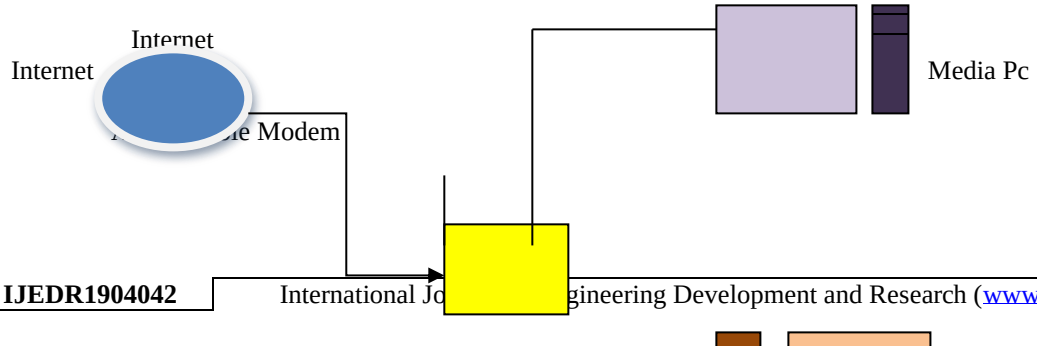
Wireless Ad-hoc network: Wireless Ad-hoc network is the collection of more than two devices which has the capability of networking. In Ad-hoc network the communication is possible within the radio range and outside the radio range. Ad-hoc network does not have any fixed infrastructure. They do not support a central system device. The mobile user in this network uses ubiquitous computing capability and information access instead of user's location. Ad-hoc network are less secured than the wired network. The router and the mobility of nodes make the network more hazarders. Wireless Ad-hoc network supports maximum of 11 mbps of speed [7].

Table 1: compares the different IEEE 802.11 standards

IEEE Standard	Frequency/Medium	Speed	Topology	Transmission Range	Access Method
802.11	2.4GHz RF	1 to 2Mbps	Ad hoc/infrastructure	20 feet indoors.	CSMA/CA
802.11a	5GHz	Up to 54Mbps	Ad hoc/infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA
802.11b	2.4GHz	Up to 11Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11g	2.4GHz	Up to 54Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11n	2.4GHz/5GHz	Up to 600Mbps	Ad hoc/infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA

WIRELESS SYSTEM ARCHITECTURE

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 are use wireless networking, also called Wi-Fi or 802.11 networking, to connect their computer 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.



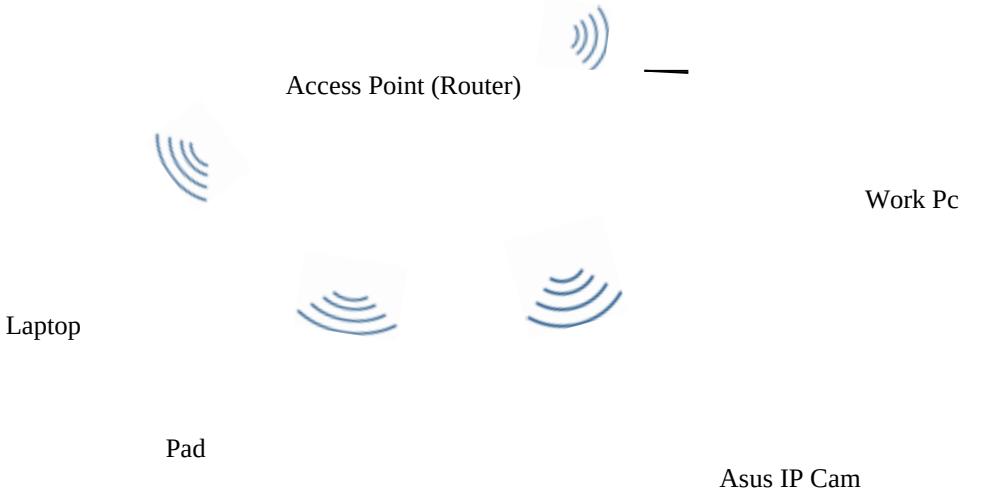


Figure 1: Wireless LAN

SECURITY THREATS AND RISKS

Low deployment costs make wireless networks attractive to users. However, the easy availability of expensive equipment also gives attackers the tools to launch attacks on the networks. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

Parking Lot Attack:

Access points emit radio signals in circular pattern, and the signals almost always extend beyond the physical boundaries of the area they intend to cover. Signals can be intercepted outside buildings, or even through the floors in multi-storey buildings. As a result, attackers can implement a "parking lot" attack, where they actually sit in the organization's parking lot and try to access internal hosts via the wireless network. If a network is compromised, attacker has achieved a high level of penetration into the network. They are now through the firewall, and have the same level of network access as trusted employees within the corporation. An attacker may also fool legitimate wireless clients into connecting to the attacker's own network by placing a unauthorized access point with a stronger signal in close proximity to wireless clients. The aim is to capture end-user passwords or other sensitive data when users attempt to log on these rogue servers.

Shared Key Authentication Flaw:

Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client. Such an attack is possible because the attacker can capture both the plaintext (the challenge) and the ciphertext (the response). WEP uses the RC4 stream cipher as its encryption algorithm. A stream cipher works by generating a key stream, i.e. a sequence of pseudo-random bits, based on the shared secret key, together with an initialization vector (IV). The key stream is then XOred against the plaintext to produce the ciphertext. An important property of a stream cipher is that if both the plaintext and the ciphertext are known, the key stream can be recovered by simply XORing the plaintext and the ciphertext together, in this cases the challenge and the response. The recovered key stream can then be used by the attacker to encrypt any subsequent challenge text generated by the access point produce a valid authentication response by XORing the two values together. As a result, the attacker can be authenticated to the access point

Denial of Service (DoS):

An attacker tampers with 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 network:

In these types of attacks an attacker goes through a list of candidate password 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.

Service Set Identifier Flaw:

Access pints come with default SSIDs. If the default SSID is not changed, it is comparatively attract more attacks from attackers since these units are regarded as poorly configured devices. Besides, SSIDs are embedded in management frames that will be broadcasted in clear text regardless access point is configured to disable SSID broadcasting or enabled encryption. By conducting analysis on the captured network traffic from the air, attacker is able to obtain the network SSID and performs further attacks.

The Vulnerability of Wired Equivalent Privacy Protocol

Data passing through a wireless LAN with WEP disabled (which is the default setting for most products) is susceptible to eavesdropping and data modification attacks. However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed, which seriously undermine its claims to security. In particular, the following attacks on WEP are possible:[8]

1. Passive attacks to decrypt traffic based on known plaintext and chosen ciphertext attacks
2. Passive attacks to decrypt traffic based on statistical analysis on ciphertexts
3. Active attacks to inject new traffic from unauthorized mobile stations.

4. Active attacks to modify data.
5. Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker's machine.

Security Services in Wireless Network:

The goal of network security is to maintain the Confidentiality, Integrity and Availability (the CIA triad) of the data and services on the network.

Confidentiality: ensures the privacy of the data, i.e. only authorized users and systems can have access to particular information. Authentication, authorization and encryption are typical mechanisms deployed to implement this, though depending on the sensitivity of the data and exposure of the systems, additional mechanisms can be brought in. there are a number of hardware and software based solutions playing a critical role in ensuring confidentiality in our networks and we will cover them in this course.

Integrity of the data ensures the accuracy and consistency, i.e. only authorized users and systems can modify the data. Furthermore, we should prevent accidental corruption of the data either unintentionally by authorized users or due to equipment malfunction. Hashes (or checksums) are often used to verify the integrity of data in transit.

Availability: requires us to maintain the normal operation and meet the quality-of-service requirements of our networks. It can be compromised not just by cyber attacks, but also by human mistakes (e.g. misconfiguration) or equipment failure. A secure network will be protected against all of these. Major effort here focuses on defending against denial of service (DoS) attacks.

Security cannot be delivered by technical measures alone; it is a combination of processes and procedures as well as technical solutions. Security is also not a one-off solution: it should be an ongoing process. One of the fundamental mechanisms in computer network and systems security is the implementation and enforcement of the organization's Security Policy. It is a relatively high level document describing the security controls of an organization. It defines several areas such as:

- **User security:** what is a secure user behavior, i.e. web browsing and email use policies, password policies
- **Device security:** end-point security such as antivirus, patch application, backup
- **Network security:** network design and implementation requirements, firewall, VPN, DMZ, Wi-Fi policies, tec.

The security policy does not need to provide specific solutions and technologies but rather identifies the mechanisms and processes that will be deployed.

Drawing up a good security policy very much depends on the industry sector, location, of the organization. One main principle in today's network security is defense in depth, that is, in order to gain access to a specific asset, the attacker will have to go through several layers of security controls and monitoring. Another one is the principle of least privilege, which specifies that access to assets should be granted only to those who need it. Where they need it and only for as long as they it [9]

CONCLUSION

Wireless network security is not an easy task; Wi-Fi network security is more difficult than wired network security. There are many protocols or standards technologies for wireless network security but every protocol has its demerits, until now there is no protocol which can provide security 100%. Many researchers are working on it and they are searching for the best protocol which can provide security as much as possible. This paper discussed wireless networks which are increasingly becoming preferred over wired networks by many users and showed the wireless security by reviewing the related standards WPANS, WLANS, WWANS, WMANS. The paper also began by offering an overview of networking and then proceeded to define wireless networking and discuss the various technologies that are used. From the discussions provided in this paper, it is clear that wireless network solutions are increasing in popularity as they become more affordable and are adopted by more people. This paper has elaborated how wireless networks provide freedom from place restriction, scalability and flexibility [10].

REFERENCES

[1] Akinola Azeez Paul & Chong Zhang Evaluate Security on the Internet Café Halmstad University, Feb, 2013

[2] Mojtaba Mohi Eldeen Adam1, Ashraf Gasim Elsid Abdallah2, Advances in Engineering and Management (IJAEM), Volume 2, Issue 2, February - 2015.

[3] Eng.Nassar Enad. GH. Muhanna, Computer Wireless Networking and Communication, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013

[4] Robert Derveloy4/17/2012, Security Issues of Ad Hoc networks, CPSC-5620 SPRING 2012

[5] Mayakrishanan, Dr. K.S.Jeya chandran, Comparison between Wireless Mesh and Adhoc
Network in Cross Layer intend Approach, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 3 issue 1 January 2016.

[6] Karthikeyan U, Security Issues Pertaining to Ad-Hoc Networks, Volume 2, Issue 9, September 2012 ISSN: 2277 128X

[7] Shikha Shukla, Meghana K M, COMPARISON OF WIRELESS NETWORK OVER WIRED NETWORK AND ITS TYPE, International Journal of Research Granthaalayah, Vol.5 (Iss.4: RACSIT), April, 2017

[8] The Government of the Hong Kong Special Administrative Region, WIRELESS NETWORKING SECURITY, Dec 2010,

[9] Basics of Network Security, Coventry University. CC BY-NC 4.0

[10] Eng.Nassar Enad. GH. Muhanna, Computer Wireless Networking and Communication, Vol. 2, Issue 8, August 2013.