A Review of Wireless Network Security

Paramjeet Kaur¹, Amanpreet Singh Dhanoa²
¹Student of M. Tech. (CSE), Rayat-Bahra University, Mohali, INDIA
²Assistant Professor (CSE), Rayat-Bahra University, Mohali, INDIA

ABSTRACT

Wireless network insecurity has become an increasing problem in the recent past days of the world of computer network. Currently, to minimize the problem in wireless network techniques like authentication and encryption is widely used to provide such barriers. The purpose of this paper is to protect a wireless network from unauthorized access. This paper focuses on the Wireless Local Area Networks (WLANs) technologies using the standard Institute of Electrical and Electronics Engineers (IEEE) 802.11.

Keywords-- Wireless network, WLAN, ad hoc, wireless sensor, network security, (IEEE) 802.11

I. INTRODUCTION

The Wireless network is a way in which one or more devices communicate with each other without a physical connection. Wireless communication is playing an important role in many areas of our society. The number of wireless phones is available in the market as compared to wired phones. It is affecting the more demand of smart-phones than PCs. Wireless LANs are commonly used at home, schools, work, and many other public places, such as cafes and malls. Wireless network connections are established by radio frequency as the medium for transporting data. Wireless local area networks (WLAN) and cell phones are the complex systems of wireless network. The device’s wireless keyboard, mouse, IR, etc. is the wireless system devices. Sometimes to make close established link between the transmitter and the receiver. Therefore, wireless network connections encounter security threats and viruses. Due to these threats and viruses the data and information transfer by the wireless network connection tends leak to unauthorized people and the security of these data and information can be leaked. To prevent that data and information from such kind of hackers used in the wireless networks. Wireless network connection will be implemented by the use of transport protocols in a VPN (Virtual Private Network) at the application level.

II. WIRELESS LOCAL AREA NETWORK

Wireless Local Area Network (WLAN) is a wireless computer network that enables people to communicate and other and access information without wires. WLAN is a group of wireless networking nodes within a limited geographic area, such as an office building or campus, that are capable of connecting through a wireless (radio) connection. Wireless networks allow people to interact with e-mail or browse the Internet from any location. Different kinds of wireless communication systems exist. They are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility. Due to the user mobility users can freely access the files through internet without any physical connection of the network on his device. The standard Institute of Electrical and Electronics Engineers (IEEE) 802.11 also defines the following two WLAN design structures or configurations, as follows:

2.1 AD-HOC WIRELESS NETWORK

An ad hoc network is the network in which a network connection is established for a single session and does not require any router [1].

From the network whenever the communication is established the node in the ad hoc organized instantly. In the ad hoc network each node directly communicates with each other node by using radio waves. The entire network of ad hoc nodes is collaborating with each other base station. An ad hoc network is local area network that builds an automatic connection to the nodes in the network. The ad hoc technology is widely used in portable computing, such as laptop, mobile phone used to access the web services, telephone calls when the user is in travelling. Development of self-organizing network decrease the communication cost. Due to design and install very simple in ad hoc network the nodes are free to move
arbitrarily and organize them at random. The topology of this network may alter quickly. The biggest challenge in ad hoc networks is to find the path between the communication end points of nodes.

![Wireless AD-HOC network](image1)

**2.2 WIRELESS SENSOR NETWORK**

A wireless sensor network (WSN) is a wireless network that consists of spatially distributed autonomous devices using the sensors to monitor physical or environmental conditions. It consists of hundreds of thousands of low-power multi-functional sensor nodes [9]. It is operating in an unattended environment, and having sensing, and communication capabilities. There are special nodes named sink (or gateways) nodes, that provides wireless connectivity back to the wired world and distributed nodes [6].

Sensor unit is a basic component of a node of the wireless sensor network. An ADC (Analog to Digital Converter), a CPU (Central processing unit), a power unit and an OPEN ACCESS Sensors 2010 are communication unit. Sensor nodes are micro-electro-mechanical systems (MEMS) that produce a measurable response to a change in any physical condition like temperature and pressure. Wireless Sensor Networks (WSNs) can be defined as a self-configured. The infrastructure of wireless sensor network is less wireless networks to monitor physical or environmental conditions, such as remote controlled heating and lighting, temperature, sound, vibration, medical monitoring, pressure, motion, automated grocery checkout, personal health diagnosis, automated automobile checks or pollutants. Sensor nodes are used to sense or measure physical data of the area to be monitored. The size of sensor nodes is very small and they consume extremely low energy are operated in high volumetric densities, and will be autonomous and adaptive towards the environment.

![Wireless Sensor network](image2)

**III. IEEE 802.11 STANDARDS**

The WLAN standards are evolving towards a faster connection while trying to cope with security problems. The first standard was published in 1997 and others have been deployed. The basic purpose of WLAN is to provide a wireless network infrastructure comparable to the wired Ethernet networks in use.

**3.1 IEEE 802.11**

The IEEE 802.11 was introduced in 1997. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbits per second. The 802.11 supported two entirely different methods of encoding (i) Frequency Hopping Spread Spectrum (FHSS) and (ii) Direct Sequence Spread Spectrum (DSSS) [10].

**3.2 IEEE 802.11b**

The 802.11b is an extension of the original 802.11 was introduced in 1999. The 802.11b operate in the same 2.4GHz frequency range, but the maximum speed is 11 Mbits per second.

**3.3 IEEE 802.11a**

The 802.11a was introduced in 1990 and amended in 2000. It has a higher frequency and a larger bandwidth allotment speed of up to 54 Mbps.

**3.4 IEEE 802.11g**

The 802.11g is an extension of 802.11b. It operates in the same 2.4-GHz band as 802.11b.

**3.5 IEEE 802.11e**

The 802.11e is standard denotes by Quality of Service (QoS) mechanisms for wireless. Quality of Service makes 802.11e standard feasible to operate bandwidth sensitive applications such as voice and video.

**3.6 IEEE 802.11n**

The 802.11n is introduced in 2009. This high-speed wireless standard can achieve wireless up to 300 Mbps by using a technique called Multiple-Input/Multiple-Output (MIMO).

**IV. SECURITY ISSUES**

Wireless security is the way in which protection from unauthorized access to computers or mobile phones by the wireless networks. Every security system must provide a packet of security functions that can satisfy the confidentiality of the system. These functions are normally referred to as the goals of the security system.

**Authentication:** It is the process in which before sending and receiving data using the system, the receiver and sender’s identity should be verified.

**Confidentiality:** Usually this function represents that how most people identify a secure system. It means that only the authenticated people can able to interpret the message (data and information) content and no one others can.

**Integrity:** It means that the content of the communicated data or information is confident to be free from any type of
modification between the endpoints (sender and receiver) [7].

**Non-Repudiation:** This function implies that neither the sender nor the receiver can falsely reject that they have sent a certain message [7].

**Availability:** Secure systems usually get attacked by the violator, which may affect their availability and type of service to their users. Such systems should provide a way to permit their users the quality of service.

**Channel:** Wirelessness involves broadcast communication which makes spy and pushing easier.

**Mobility:** Although not all wireless devices are mobile, wirelessness, by its very nature, enables mobility. In wireless communication, the physical connection is replaced by logical association [2].

**Resources:** Some modern high-end wireless devices (e.g. Smart-phones) have fast processors and they run on actual operating systems, thus blurring the distinction between them and laptops. However, most wireless devices are still Resource-constrained [2].

**Accessibility:** While some devices are personal and usually attended by their owners, others (e.g., sensors or robots) are generally left unattended and are placed in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks [2].

**V. CONCLUSION**

As wireless networks are mostly used in homes, offices and public areas, therefor increasing threats and un-authority to secure. They are three basic technology components of wireless networks. (Clients, access points, and the transmission medium) and described various commonly available actions that could be used to reduce those risks. This research paper will conclude that to be directed towards those who are not IT minded in order to raise their awareness towards making their own personal efforts in raising security and at the same time prevent them from being the point of entry for hackers into their personal networks.

**REFERENCES**


[2]. Di Ma “Security and Privacy in Emerging Wireless Networks”.


