Article can be accessed online at http://www.publishingindia.com

Wireless Network Security Spread Spectrum Techniques

Rajinder Singh*

Abstract

Wireless LANs enable users to communicate without the need of wires. In this technology two or more devices use radio frequency to transfer and receive data over air. WLAN network uses a wireless Access Point (AP) to transmit and receive data from users. The major difference between wired LAN and WLAN is WLAN transmits data by using radio waves instead of transmitting electrical signals over a wire. Nowadays wireless networks are gaining popularity as one can use them in many areas such as in classrooms or in workplace due to flexibility and portability of wireless devices. Since wireless devices transmit radio signals over a wider area, so security become major concern. Anyone with proper Wi-Fi device and wireless NIC can intercept radio signals from the nearby wireless network. Therefore, it is important to enhance the network security in order to protect the information of the network. Many security protocols have been designed to protect the wireless networks. But later it has been found that theses protocols were not able to provide complete security. In this paper some of threats that can be made at physical layer and countermeasure using spread spectrum techniques are discussed.

Keywords: Security, Protocol, Threat, Spread Spectrum

1. Introduction

Main advantages of Wireless networks are that they provide convenience, mobility, and are less cost effective than the wired networks. Nowadays following different WLAN standards are used: 802.11, 802.11a, 802.11b, 802.11g and 802.11n. 802.11 apply to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band. 802.11 use either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). IEEE 802.11a operates in the 5GHz band and provides data rates up to 54Mbps. 802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme. 802.11b operates in the 2.4GHz band and data rate is up to 11Mbps. It uses DSSS modulation scheme. 802.11g also operates in 2.4GHz band and provide data rates up to 54 Mbps. The 802.11g uses both OFDM and DSSS modulation schemes. 802.11n operates in 2.4 GHz band and provides data rates 100Mbps to 200 Mbps. It uses OFDM encoding scheme [8].

1.1. Main Components of The Wi-Fi Network

Main components of Wireless Networks are: a) Wi-Fi client or any Wi-Fi enabled device b) Access Point or Wi-Fi hot spot c) Routers or modems. Router or modem provides actual internet connection to the internet with the help of cables or wires. Wi-Fi clients transfer and receive radio signals. They also convert radio signals into digital data.

Wi-Fi clients connect to network with the help of access point [2]. An access point is used to connect Wi-Fi devices to local area network. Access points convert and control the sending of data packets. It can connect one or many wireless devices to a wired LAN.

A computer's or laptop's wireless network interface card transfer digital data into radio signals. These radio signals are received by Access Point. Then these signals are converted into digital data. Then router sends the data to the Internet using a physical connection. The same process also repeated in reverse, with the Access Point

* Assistant Professor, Department of Computer Science & Applications, Swami Sarvanand Giri Regional Centre, Panjab University, Hoshiarpur, Punjab, India. E-mail: rajinderid@gmail.com

receiving data from the Internet; transfer it into radio signals and send it to the computer's or laptop's wireless network interface card [9].

2. Physical Layer Threats

Threats are entities that can attack networks through system vulnerabilities. An attack is an attempt to get the information of wireless network. It also attempts to change the operation of the wireless network resources. Examples of threat are hackers, viruses and spywares that can cause disturbance in the network. Vulnerability is a weakness or flaw in operating system or software that can be exploited by a threat. Some examples are wireless networks not using encryption, weak passwords and Access Point sending wireless signals outside the building [1].

Some of the physical layer threats are given below.

2.1. Accidental Associations

Wireless Access Point uses radio waves to transfer data to end user. Radio waves can travel long distances, and so they can penetrate buildings, wall, doors and floors easily. Moreover radio waves are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically. So these signals can enter into another organization's network and can connect with their wireless local area network. This is called accidental associations. So one can use this flaw to connect to another organization's wireless network with the help of a Wi-Fi device [3].

2.2. Jamming

Jamming mean to break up the wireless communication by transmitting the radio signals. Nowadays some of the common devices that operate on the 2.4 GHz band are available easily. Some of them are Cordless Phones, Bluetooth Devices, Car Alarms and microwave ovens. They can also be used by attacker to jam the wireless network. Jamming is also used to launch Denial of service attack at the physical layer.

2.3. Traffic Analyzing

In this case attacker can determine the load on the communication medium by the number and size of packets being transmitted. The attacker only needs a wireless card operating in listening mode and software such as Kismet and Wireshark to count the number and size of the packets being transmitted. A helical directional antenna provides an increased range at which the attacker may analyze the traffic. The attack primarily identifies that there is activity on the network. Attacker can also identify the physical location of wireless access points (APs) in the surrounding area with the help of traffic analyzing. Attacker can also identify the type of protocols being used in the transmissions [4]. After analyzing the wireless traffic attacker can launch another types of attacks on the network.

One countermeasure against Traffic Analyzing Attack is using strong encryption keys.

3. Spread Spectrum Techniques

Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is intentionally changed. Narrow band signal is transmitted on a wider bandwidth. In wireless local area networks (WLAN), Access Points (APs) and stations use following technologies for signal transmission: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Orthogonal frequency Division Multiplexing (OFDM).

Direct-sequence spread spectrum (DSSS) is a modulation technique in which the transmitted signal takes up more bandwidth than the information signal. In this technique original data is multiplied by a noise like signal which is a pseudorandom sequence of 1 and -1 values. Then this noise-like signal used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence. This process is known as de-spreading. For de-spreading to work correctly, the transmitter and receiver must synchronize their sequence [5] [10].

In Frequency Hopping Spread Spectrum (FHSS) the data is transmitted on a range of frequencies. These frequencies are changed several times during the transmission. In this

technique original data is split into small units and then transmitted on these channels in a random pattern known only to the transmitter and receiver. In frequency hopping spread spectrum a transmitter hops between available frequencies according to a specified algorithm. Both the transmitter receiver operates in synchronization. A short burst of data is transmitted on a narrowband, and then the transmitter tunes to another frequency and transmits again. Therefore in frequency hopping there is repeated switching of frequencies during radio transmission. Main characteristic of spread spectrum is the presence of a code or key, which must be known in advance by the transmitter and receiver [6].

Orthogonal frequency division multiplexing (OFDM) is a technique in which digital data is encoded on multiple carrier frequencies. In OFDM signal is split into many independent channels and then modulated by data. [11].

4. Physical Layer Threst and Spread Spectrum Techniques

a. Jamming can be avoided by using spreading techniques. In case of Jamming an attacker uses equipment or transmitter designed to block radio transmissions on a given frequency. But in FHSS signal does not stay in one place of the band so FHSS can easily confuse a jammer. It can also retransmit garbled data that has been corrupted by interference during other hops. In case of interference on one channel, data transmission is blocked. The transmitter and receiver hop to the next channel and the transmitter resends the data packet. Frequency hopping technology is best for transmitting small data packets in high interference environments.

   DSSS also give resistance to intended or unintended jamming because it uses low power density, making it harder to detect. DSSS is best for transmitting large data packets in a low to medium interference environment [12].

   In case of DSSS intentional or intentional interference are rejected because they do not contain the spread-spectrum key. Only the desired signal which has the key will be seen at the receiver end. To an unintended receiver, DSSS appears as low-power wide-band noise and is ignored by most narrowband receivers [13].

b. Accidental association can also be avoided using spread spectrum technique. Wireless networks use two basic types of antennas for sending the radio signal: Omni-directional and Directional. Omni-directional antenna radiates signals equally in all directions. Directional antenna transmits the signals in one specific direction. So organizations should try to use Directional antenna instead of Omni-directional antenna.

c. To some extent eavesdropping and Traffic Analyzing threat can also be avoided using spreading techniques. The spreading code in DSSS systems or the frequency-hopping pattern in FHSS systems is only known to sender and receiver. So if an attacker intercepts the signal then without code it will appear as noise. Since Spread Spectrum techniques spread the original signal over a wider band therefore power spectral density of the transmitted signal is very small as compared to the noise level. So an attacker is unable to determine the signal whether it exists or not [7].

5. Conclusions

In this paper some of the threats that can be made at physical layer are discussed. Then various spread spectrum techniques that are used to avoid these threats are also discussed.

Under normal conditions both spread spectrum techniques FHSS and DSSS work well. But in case of presence of large interference DSSS may stop operating but FHSS will hop to next frequency. So FHSS will degrade slowly.

So organizations should first consider external environment before taking any decision regarding installation/implementation of any spread spectrum technique.

References

1. Beaver, K. & Peter, T. & Hacking, D. (2005). *Wireless Networks for Dummies*. (pp. 9-11). Wiley Publishing Inc.
2. Stallings, W. (2007). *Computer Networking with Internet Protocols and Technology*. (pp.555-556). Pearson Education,Inc.
3. Heather, D. (2005). Lane, Security Vulnerabilities and Wireless LAN Technology.

4. www.itsce.gov.cn/docs/20090507161931121853.pdf
5. http://searchnetworking.techtarget.com/definition/direct-sequence-spread-spectrum
6. http://searchnetworking.techtarget.com/definition/frequency-hopping-spread- spectrum
7. http://searchnetworking.techtarget.com/definition/frequency-hopping-spread-spectrum
8. http://en.wikipedia.org/wiki/Spread_spectrum
9. http://www.javvin.com/protocolWLAN.html
10. http://computer.howstuffworks.com/wireless-network1.htm
11. http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum
12. http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing
13. http://www.bannerengineering.com/
14. http://www.maximintegrated.com/app-notes/index.mvp/id/1890