Security In Wireless Local Area Network

Okemiri Henry Anayo
Department of Computer Science/Informatics
Alex Ekwueme Federal University Ndufu-Alike
Ebonyi State, Nigeria
henry.okemiri@funai.edu.ng

Oketa Christian kelechi
Department of Computer Science/Informatics
Alex Ekwueme Federal University Ndufu-Alike
Ebonyi State, Nigeria
callchris@yahoo.com

Afolabi Idris Yinka
idrizbaba@gmail.com

Ekeh Godwin E
egodwinekeh@yahoo.com

***Abstract*—A wireless local area network is a wireless access point that provides internet access to network devices in public locations such as schools, downtown centers, cafes, airports and hotels. But just with most technologies, network is not without its own challenges. Some of these includes: Unauthorized Clients, Renegade Access Points, Interception and monitoring of wireless Traffic, Access Point Clone, Traffic Interception etc. This paper deals with this wireless local area security technologies and aims to exhibit their potential for integrity, availability and confidentiality. It provides a thorough analysis of the most WLAN packet data services and technologies, which can reveal the data in a secure manner. Wireless LANs are now also capable of supporting time-sensitive services such as voice and video. These services have stringent service requirements from the network infrastructure. These requirements supersede the requirements of general traffic data. The protocols used for such services are Enhanced Distributed Coordination Function(EDCF) and Hybrid Coordination Function(HCF). To get a better understanding of these protocols, we will also understand Distributed Coordination Function (DCF).**

Keywords—Wireless LAN, IEEE 802.11, Enhanced Distributed Coordination Function, Distributed Coordination Function

A wireless LAN is a flexible data communications system implemented as an extension to or as alternative for a wired network. Using Radio frequency (RF) Technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. Wireless LAN users can access shared information without looking for a place to plug in, and network administrators can set up networks without installing physical cables. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications take place “through the air” using Radio Frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it thereby compromising confidentiality.

A Wireless Local Area Network (WLAN) links two or more devices using a wireless communication method. It usually provides a connection through an Access Point (AP) to the wider internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Just as the cordless telephone frees people to make a phone call from anywhere in their home, a WLAN permits people to use their computers anywhere in the network area, such as an office building or corporate campus. Due to their ease of installation and the increasing popularity of laptop computers, WLANs have been widely deployed in the past two decades.

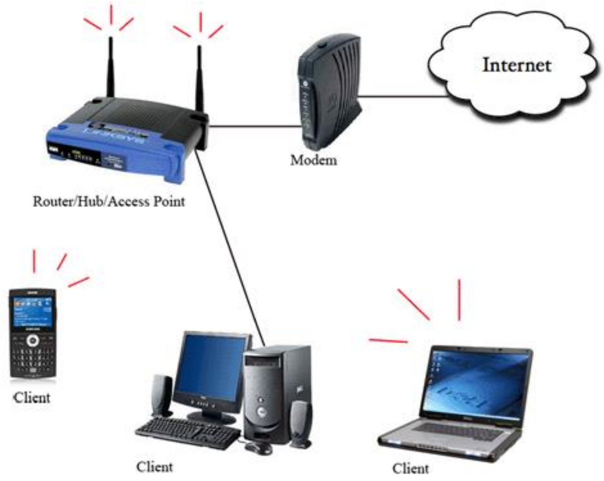


Figure 1.1:Wireless Local Area Network.

METHODS OF ACCESSING WIRELESS LANS

Wardriving is perhaps the most common method hackers use to locate unsecured wireless networks. Wardriving involves driving around neighborhoods or near business with notebook computers searching for unsecured wireless networks. Hackers use special software to locate and access these networks. Apartment complexes and residential neighborhoods can offer dozens of unsecured networks. Restaurants and coffee shops that offer wireless internet services could also provide a convenient access point to your computer while you are enjoying your lunch. (Kelly, 1999).

WIRELESS SECURITY

Donald (2011), wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or WiFi protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP. Many laptop computers have wireless cards pre-installed. However, wireless networking is prone to some security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Detection Systems (WIDS) are commonly used to enforce wireless security policies.

MODES OF UNAUTHORIZED ACCESS

The modes of unauthorized access to links, to functions and to data is as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new modes of operation will create new options of threatening. Hence, prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply (EDITH, 206)

ACCIDENTAL ASSOCIATION

Violation of security perimeter of a corporate network can come from a number of methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred. However,it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network. Accidental association is a case of wireless vulnerability called “misassociation”. Misassociation can be accidental, deliberate or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker’s APs.

AD-HOC NETWORKS

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

IEEE 802.11

Since its introduction in 1997, IEEE 802.11 has become the dominant WLAN standard [54]. IEEE 802.11 is a member of the IEEE 802 family, which is a series of specifications for Local Area Network (LAN) technologies. IEEE 802 specifications are focused on the two lowest layers of the OSI 7-layer model1, because they incorporate both physical and data link components. All IEEE 802 networks have both a MAC and a Physical (PHY) component. The MAC layer is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY layer.

IEEE 802.11 is a set of standards, which specifies WLAN computer communication in the 2.4 and 5 GHz frequency bands. IEEE 802.11 includes all over-the-air modulation techniques that use the same basic protocol. The original version of the IEEE 802.11 standard was released in 1997 and clarified in 1999. It specified two bit-rates of 1 and 2 Mb/s, plus a Forward Error Correction (FEC) code. It also specified three alternative PHY layer technologies: diffuse InfraRed (IR) operating at 1 Mb/s, Frequency-Hopping Spread Spectrum (FHSS) operating at 1 Mb/s and 2 Mb/s; and Direct-Sequence Spread Spectrum (DSSS) at 1 Mb/s and 2 Mb/s. The latter two radio technologies use microwave transmission over the Industrial Scientific Medical (ISM) frequency band at 2.4 GHz. In this thesis, we are interested in 5 members in the IEEE 802.11 family, which are IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11e and IEEE 802.11s. The IEEE 802.11a standard, released in October 1999, uses the same data link layer protocol and same format as the original IEEE 802.11 protocol, but an Orthogonal Frequency-Division Multiplexing (OFDM) based air interface at the PHY layer [54]. It operates in the 5 GHz band with a maximum bit rate of 54 Mb/s. Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively lightly used channel of 5 GHz gives IEEE 802.11a some significant advantages. However, this high carrier frequency also brings some disadvantages. Due to their smaller wavelength, the IEEE 802.11a signals will be absorbed more heavily by walls and other solid objects in their path. As a result, the IEEE 802.11a signals cannot penetrate as far as those of the IEEE 802.11 b/g that operate in the frequency band of 2.4 GHz. Consequently, the effective overall range of the IEEE 802.11a rates is less than that of the IEEE 802.11 b/g rates.

IEEE 802.11 in the MAC Layer

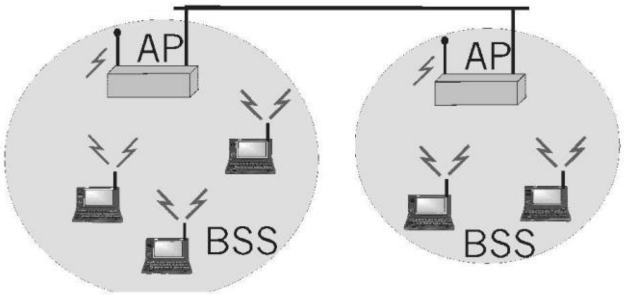
The IEEE 802.11 protocol covers the MAC and PHY layers. The standard currently defines a single MAC which interacts with three PHYs (IR, FHSS and DSSS). The MAC Layer defines two different access methods, the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

Distributed Coordination Function

The basic access mechanism, called the DCF, is a Carrier Sense Multiple Access with Collision Avoidance mechanism (CSMA/CA) [119]. A CSMA protocol works as follows. A station with a packet to transmit senses the medium. If the medium is busy (i.e. any other station is transmitting) then the station postpones its transmission to a later time. If the medium is sensed to be free then the station transmits. These kinds of protocols are effective when the medium is not heavily loaded since it allows stations to transmit with minimum delay. There is, however, always a chance that stations simultaneously sense the medium as being free and transmit at the same time, which causes a collision. These collision situations must be identified so the MAC layer can retransmit the packet by itself and not by upper layers, which would cause significant delay. In an Ethernet network this collision is sensed by the transmitting stations which go into a retransmission phase based on a binary-exponential random back-off algorithm.

While these collision detection mechanisms are a good idea for wired LANs, they cannot be used in a WLAN environment for two main reasons. First, implementing a collision detection mechanism would require the implementation of a full duplex radio capable of transmitting and receiving at once, an approach that would increase the price significantly. Second, in a wireless environment we cannot assume that all stations hear each other, which is the basic assumption of the collision detection scheme, and the fact that a station wants to transmit and senses the medium as free does not necessarily mean that the medium is free around the receiver area. In order to overcome these problems, IEEE 802.11 uses a Collision Avoidance (CA) mechanism together with a positive acknowledgement scheme [119]. First, a station wanting to transmit senses the medium. If the medium is busy then it defers the transmission. If the medium is free for a specified time (called distributed inter frame space, DIFS), then the station is allowed to transmit. Second, the receiving station checks the integrity of the received packet and sends an acknowledgment packet (ACK). Receipt of the ACK indicates to the transmitter that no collision occurred. If the sender does not receive the ACK then it retransmits the packet until it receives an ACK packet. If the transmission of a packet experiences a number of consecutive failures, the sender should discard this packet. However, the collision avoidance mechanism is not effective in a network with hidden nodes. Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes. In order to reduce the probability of two stations colliding because of the hidden node problem, the standard defines a virtual carrier sense mechanism. A station wanting to transmit a packet _rst transmits a short control packet called Request To Send (RTS), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective ACK). The destination station responds (if the medium is free) with a response control packet called Clear To Send (CTS), which includes the same duration information. All stations receiving either the RTS and/or the CTS, set their virtual carrier sense indicator (called NAV for Network Allocation Vector) with the given duration. During this period, these stations must refrained from accessing to the medium. This mechanism reduces the probability of a collision on the receiver area by a station that is `hidden' from the transmitter to the short duration of the RTS transaction because the station hears the CTS and `reserves' the medium as busy until the end of the transmission. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station). It should also be noted that, due to the fact that the RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted. This is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transaction. This is controlled per station by a parameter called RTS/CTS threshold.

The basic building block of a WLAN network is the Basic Service Set (BSS), which is simply a group of stations that communicate with each other. Communication takes place within a somewhat fuzzy area, called the `basic service area', defined by the propagation characteristics at a given rate in the medium. When a station is in the basic service area, it can communicate with the other members of the BSS. Generally, BSSs come in three avors: independent networks, infrastructure networks and extended service areas.



Example of wireless infra-structure fig.1.2

In a typical WLAN configuration, a transmitter/ receiver device, or Access Point(AP), connects to the wired network from a fixed location using standard Ethernet cable. The access point receives, buffers and transmits data between the components of the WLAN (laptops, printers, handheld devices and other wireless equipment) and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than 100 to several hundred feet. The access point can be installed anywhere in the facility as long as good radio coverage is achieved. Basic Service Set(BSS) is a set of 802.11 compliant stations that operate as a fully-connected wireless network. Generally, BSS comprises to an Access Point and a number of stations associated with it. Now there arises a need to have a common protocol between the wireless client and the access points. 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

IEEE 802.11B SECURITY FEATURES

The security features provided in 802.11b standard are as follows:

a) SSID –Service Set Identifier SSID acts as a WLAN identifier.

Thus all devices trying to connect to a particular WLAN must be configured with the same SSID. It is added to the header of each packet sent over the WLAN (i.e. a BSS) and verified by an Access Point. A client device cannot communicate with an Access Point unless it is configured with the same SSID as the

Access Point.

b) WEP - Wired Equivalent Privacy : According to the 802.11 standard, Wired Equivalent Privacy (WEP) was intended to provide “confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy”. IEEE specifications for wired LANs do not include data encryption as a requirement. This is because approximately all of these LANs are secured by physical means such as walled structures and controlled entrance to building etc. However no such physical boundaries can be provided in case of WLANs thus justifying the need for an encryption mechanism. WEP provides for Symmetric Encryption using the WEP key. Each node has to be manually configured with the same WEP key. The sending station encrypts the message using the WEP key while the receiving station decrypts the message using the same WEP key. WEP uses the RC4 stream cipher.

c) MAC Address Filters

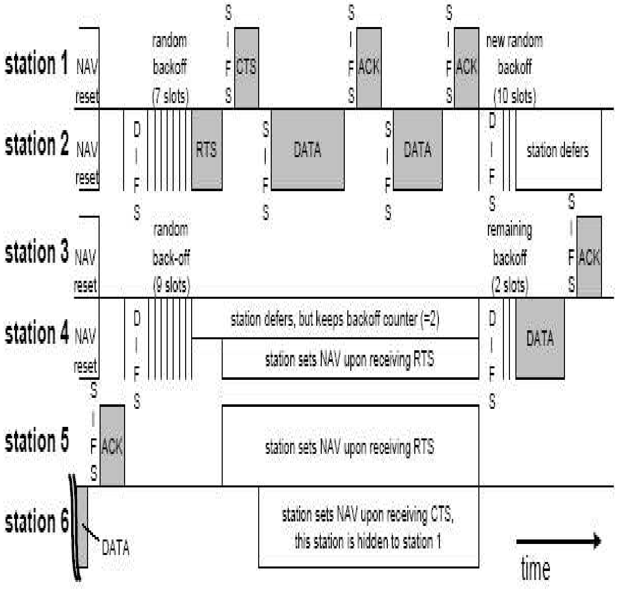
In this case, the Access Point is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with the Access Point. This scheme provides an additional security layer.

ENHANCED DCF (EDCF) PRIORITY SCHEME

The contention-based channel access function of IEEE 802.11e is EDCF, in which multiple queues (up to 8) are used for different priorities (up to 8). Priorities are achieved by differentiating the arbitration inter-frame space and the initial window size. The traffic is classified into 8 priority classes: *i* □□0,.7 . For the priority *i* class, the minimum backoff window size is min*CW* [*i*] , and the arbitration interframe space is *AIFS*[*i*] . If the priority *i* class has a lower priority than the priority *j* class, we have min min *CW* [*i*] ≥□*CW* [*j*] , and *AIFS*[*i*] ≥□*AIFS*[*j*] , and at least one of above inequalities must be a real inequality. In other words, EDCF adopts *AIFS*[*i*] (*i* □□0,1,.,7) and min*CW* [*i*] (*i* □□0,1,.,7) instead of DIFS and min *CW* , respectively. If one class has a smaller *AIFS* or min *CW* , the class’s traffic has a better chance to access the wireless medium earlier.

Distributed Coordination Function(DCF)

DCF works on a listen-before-talk scheme, based on the Carrier Sense Multiple Access (CSMA) scheme. Any station first detects whether there is any transmission going on in wireless medium (listen), and only on finding it free it transmits (speak). However, if two stations detect the medium to be free at the same time, collision can take place. Thus, 802.11 defines a Collision Avoidance (CA) mechanism. As per this mechanism, everyone has to wait for a random time before speaking to avoid collision i.e. a station performs a random back-off procedure before starting. Every station has to keep sensing the channel for a random time after detecting the channel being idle for a minimum duration called DCF InterFrame Space (DIFS).


station 1
NAV reset
random backoff (7 slots)
SIFS
CTS
SIFS
ACK
SIFS
ACK
new random backoff (10 slots)
station 2
NAV reset
DIFS
RTS
SIFS
DATA
SIFS
DATA
DIFS
station defers
station 3
NAV reset
random back-off (9 slots)
remaining backoff (2 slots)
SIFS
ACK
station 4
NAV reset
DIFS
station defers, but keeps backoff counter (=2)
station sets NAV upon receiving RTS
DIFS
DATA
station 5
SIFS
ACK
station sets NAV upon receiving RTS
station 6
DATA
station sets NAV upon receiving CTS, this station is hidden to station 1
time

DCF with RTS/CTS mechanism fig.1.3

REFERENCES

[1] A. Akella, G. Judd, S. Seshan, and P. Steenkiste. Self-management in chaotic wireless deployments. In 11th International Conference on Mobile Computing and Networking, 2005.

[2] A.A. Ali and K. Alkhudairi. BER for M-QAM with space-time transmit diversity in Nakagami

[3] and Rician fading channelss. Technical report, King Saud University, 2009.

[4] Dr. Gurjeet Singh "Performance and Effectiveness of Secure Routing Protocols in

[5] MANET" Global Journal of Computer Science & Technology" Vol 12, Issue 5, 2012.

[6] Gregori. E. Cali. F, Conti. M. Ieee 802.11 wireless lan: capacity analysis and protocol enhancement. In INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 1998.

[7] Kelly S., and Vincent F. (1999). A review of wireless Network Management System for private and public sectors, Jos: Fatima & Amina Press Nigeria LTD.

[8] Y. Barowski, S. Biaz, and P. Agrawal. Towards the performance analysis of IEEE 802.11 in

[9] multi-hop ad-hoc networks. In Proceedings of IEEE Wireless Communications and Networking Conference, 2005.

[10] Young, Chrisher. E. (2005). Computer Application and Wireless network Management system. Ibadan: M. C. &Jojo Publication limited.

[11] S. Mangold, S. Choi, P. May, O. Klein, G. Hietz and L. Stibor, "IEEE 802.11e wireless lan for quality of service," *Proceedings of the European Wireless*, 2002 Feb.

[12] J. Weinmiller, M. Schlager, A. Festag, and A. Wolisz, "Performance study of access control in wireless LANs IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN," Mobile Networks and Applications, vol. 2, pp. 55-67, 1997.