WIRELESS LAN-802.11
Sushil Kumar
Scientific Officer-E, Department of Atomic Energy,
Heavy Water Board, India
sushilkumaret@gmail.com

Publication History
Manuscript Reference No: IRJCS/RS/Vol.07/Issue07/JLCS10081
Received: 11, July 2020
Accepted: 13, July 2020
Published: 15, July 2020
DOI: https://doi.org/10.26562/irjcs.2020.v0707.001
Peer-review: Double-blind Peer-reviewed
Editor: Dr.A.Arul Lawrence Selvakumar, Chief Editor, IRJCS, AM Publications, India
Copyright: ©2020 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: Communication is the basic need and back-bone for development of any society. Societal development and advancement in the electronics & technology led to the development of Wireless based Systems & has become vital for the modern existence. Wireless Local Area Network (WLAN) is the best example for the same. Popularity of the Wireless Local Area Networks (WLANs) are in increasing trend as they are fast, flexible, cost effective, and easy to use. Application & uses of the WLAN has led some security challenges also & choice of security protocol is one of the typical tasks. In general, any information system incorporating wireless technology should fulfill some basic security objectives. The typical taxonomy of security properties can be described by confidentiality, integrity, and availability (CIA). In wireless communication, data rate is increasing drastically due to advancement in technology at a massive scale. In this paper, we review and summarize IEEE 802.11 protocol architecture, component of WLAN, and security issues in WLAN etc.

Keywords: Wireless Security, Wi-Fi, WEP, TKIP, CIA, Ad-hoc, FCC, MAC, SSID, CRC etc.

I. INTRODUCTION

Communication is the basic need and back bone for development of any society & plays an important role in everybody's life in all the days. Calling present era, as communication technology era shall not be a hype. We are living along with the machines for the ease of comfort & getting our jobs done directly through the machines or in some way controlled by machine or computers. All this is made possible by development in electronics, information and communication technology. Advancement & Technology development in the electronics led to the birth of wireless Communication. Usages of Wireless technology have helped to explore the networking in more simple way by allowing of sharing the resources simultaneously with reduced wired network. Continual improvement in usage of wireless network infrastructure raised the need for strong safety mechanisms. Wireless networks have no inherent physical protection, as physical connections between devices have been replaced by logical associations.

Figure-1
Though wireless networks and wired one face similar vulnerabilities to attack, however due to the inherent nature of wireless media there are some fundamental differences between the nature of the threats and their detection. On a wired network, attacks can originate at remote locations of the wire, whereas the attacking points on the wireless network need to be local and within the range of the attacker’s wireless network devices. In any System, Security is based on CIA Triad; it is the base line for implementing the security.

CIA stands for Confidentiality, Integrity & Availability. CIA & its application while developing the WLAN standards are considered. Keeping all the above, a group of alliances was formed named as wi-fi alliances in the starting of 90’s.

In the year 1999, IEEE has developed & introduced the standard named as 802.11 along with security protocol & mechanism for wireless LAN. The 802.11 WLAN standards has given focus on bottom two layers of the OSI (Open System Interconnection) ie. The Physical layer (PHY) and medium access control (MAC) layer.

II. DEVELOPMENT OF IEEE 802.11

A wireless LAN (WLAN) is defined as ‘a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure’. Standards provide a model & guidelines for development & better usage, considering the same IEEE-802.11 project was developed for WLAN. During development of IEEE 802.11 project, focus was given on bottom two layers of the OSI (Open System Interconnection) ie. The Physical layer (PHY) and medium access control (MAC) layer, as behaviour of the signal for wireless medium was quite different compared to wire one. During the development of IEEE802.11 standard, initially it was thought that wireless medium can be considered as another physical layer of one of the available standards (eg 802.3, 802.4, 802.5 etc). The first protocol standard which was considered for this was IEEE’s most prominent standard 802.3.

However later findings showed that the behaviour of the radio medium is quite different compare to the conventional well behaved wired one. As in wireless medium, signal gets attenuated as distance increases, collisions could not be detected. Hence, 802.3’s carrier sense multiple access with collision detection (CSMA/CD) could not be applied. The next protocol standard considered was 802.4. At that point of time, its coordinated medium access i.e. the token bus concept was believed to be superior to 802.3’s contention-based scheme. However later it became obvious that token handling in radio networks was more difficult. The standardization body realized the need of a wireless communication standard that would have its own very unique MAC.

COMPONENTS OF WLAN

Major components of the IEEE 802.11 are as follows:

Base Stations or Stations (STAs):
Instruments or Devices(STAs)having computing capabilities, equipped with wireless network interfaces and communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishment of connections between STAs and AP goes through various phases and generally STAs are controlled by AP.
Access Points: The most important function of an Access point is bridging, which increases the effective range of wireless network. The frame which is used for communication in a wireless network needs to be converted to another type for it to be delivered to the rest of the world. It allows wireless devices to get connected to a wired network.

Wireless medium: A wireless medium is through which data /communication takes place from one station to another. The architecture allows a number of physical layers to be developed in order to support 802.11. During start of development of 802.11 only 1 Infrared and 2 Radio frequency (RF) in physical layers were standardized but RF proved to be more popular.

Distributed System: It is basically infrastructure used to connect multiple Access Points, which may form a large coverage area to communicate with one another to track the movements of the mobile stations. It is implemented as combinations of a distributed system medium and bridging engine. When configuring the distributed WLAN, multiple Access Points are configured with the same SSID to make a single logical network within a single Layer2 broadcast domain. Distribution System is commonly known as backbone of the network.

III. IEEE 802.11 STANDARD DEFINES THREE TYPES OF WIRELESS NETWORK TOPOLOGY: IBSS, BSS, AND ESS:

1. Independent Basic Service Set (IBSS), i.e., ad-hoc network: "An ad-hoc network is a network composed solely of stations within the mutual communication range of each other via the wireless medium."In ad-hoc network, nodes typically don’t require any administrator. Networked nodes share their resources without a central server. In ad hoc networks, several wireless nodes join together to establish a peer-to-peer communication as shown in Figure 3.

   Figure-3: Ad-hoc wireless network

As noted in the 1999 edition of the 802.11 specifications, "The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent". To achieve a more permanent wireless network, with larger communication range, infrastructure modes are often used.

2. Basic Service Set (BSS): A BSS is "a set of stations controlled by a single coordination function". A BSS, commonly referred to as an infrastructure network, consists of a single access point and a number of end nodes as shown in Figure 4.

   Figure-4: wireless LANs with infrastructure (Basic Service Set)

All the communication between any two nodes has to pass through the AP. The coverage area is greatly increased as compared to an IBSS. In wireless LANs with infrastructure, there is a high-speed wired or wireless backbone. Wireless nodes access the wired backbone through access points (see Figure 4). These access points allow the wireless nodes to share the available network resources efficiently. Typical star topology resembles access points in hub.
3. **Extended Service Set (ESS):** ESS is "a set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs". ESS consists of multiple BSSs each having a single access point. The access point in each BSS is connected to a distribution system that is usually a wired Ethernet network. An ESS is a hybrid of wireless and wired LANs, and extends a wireless station’s connectivity beyond its local access point.

![Figure-5: wireless LANs with ESS](image)

### IV. IEEE-802.11 PROTOCOL ARCHITECTURE

The IEEE 802.11 protocol architecture is shown in Figure-6. The 802.11 standards specify two lowest layer of the OSI network model which are physical and data link layers. The bottom most layer, the physical layer, specifies the physical & electrical characteristics of the system eg topology operating frequency bands & the supported data rates etc. Next layer is Data Link Layer which defines the access control methodologies, protocol multiplexing & hop to hop flow and error control.

![Figure-6](image)

**Physical (PHY) Layer**

The IEEE 802.11 defined basically spread spectrum techniques, operating frequency as 2.4GHz, called as FHSS & DSSS, Infrared passive reflection and OFDM were also added to the layer with the aim of increasing the aggregate throughput of the network. IEEE 802.11 standard defines PHY layers namely:

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- IR (Infrared)
- OFDM (Orthogonal Frequency Division Multiplexing Modulation)

Details of the above mentioned various layers are not discussed in this present paper.
Medium Access Control (MAC) Layer
802.11 specify two types of services i.e. contention based & contention free. Contention based services uses DCF (Distributed Coordinated Function) & Contention free services use PCF (Point Coordinated Function). The access methods used in Infrastructure mode are Distributed Coordination Function (DCF) and Point Coordination Function (PCF), while Distributed Coordination Function (DCF) is the access mode used in Ad-hoc Mode.

Distributed Coordination Function:
It is the basic access method in 802.11 at MAC layer protocol for the ad hoc networks. It uses Carrier sensing CSMA/CA protocol (Carrier Sense Multiple Access with Collision Avoidance). Wireless communication in general taken place via radio medium, it behaves quite different compared to the conventional wired medium. As in radio medium signal attenuation takes place even over short distances, due to that collisions detection is quite tough. Which shows, 802.3’s carrier sense multiple accesses with collision detection (CSMA/CD) could not be applied?

CSMA/CD cannot be used in wireless systems, as is used in Ethernet, wired LAN due to the following reasons:
• Wireless system are half duplex system
• Signal strength
• Hidden terminal.

In CSMA/CA, The medium is sensed for a period greater than Distributed Inter-Frame Space and if it is found to be idle, the station is allowed to transmit a packet in the alternate case the station computes a back off time which is randomly generated called the back off time which is in the range of 0 and Contention Window (CW). This back off timer gets decremented periodically, upon reaching the value of 0 the station is allowed to access the Network again. If acknowledgement is not received the station assumes a collision has taken place and re-schedules a transmission by re-entering the back off process.

Point Coordination Function:
It employs the Time Division Multiplexing (TDM) technique & works on master slave principle. In PCF, transmission time is divided into poll slots for the stations in a network. Any stations, slave, can transmit data only after receiving a polling frame from the point coordinator. The point coordinator, the master, decides which station must be polled for data transmission. PCF is used for infrastructure configuration only & in PCF, There is no delay caused due to collision as the PCF provides bounded delay. In PCF mode, access point can be configured optionally. Stations are free to decide whether to employ polling or not in spite of enabling the above mode.

V. SECURITY OF 802.11 WIRELESS LANS
Working group, IEEE 802.11, defined a family of specifications for wireless LAN technology with a goal “to provide wireless LAN with security level equivalent to the wired LANs” and also has identified several services to provide a secure operating environment.

![Diagram of wireless network security](Figure-7)

Wired Equivalent Privacy (WEP) protocol was incorporated in 802.11 to provide security services to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure-7. WEP is an optional security mechanism for protecting wireless networks (IEEE Computer Society LAN MAN Standards Committee, 1999). WEP was included in clause 8.2 of the first version of IEEE 802.11 and has remained unchanged in newer versions of IEEE 802.11 b, 802.11g, and 802.11a for ensuring compatibility amongst different versions. At MAC level encryption is implemented, WEP is chosen for this and is supported by most wireless solutions.

VI. BUILT-IN 802.11 SECURITY ASPECT
WEP (wired equivalent privacy) is the protocol which provides data security in WLAN (802.11), the same way as it is in the wired networks.
Wireless network system enables all users within the network range to receive data if they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on the second layer of OSI model and, in this way, provide the data protection during the transmission. In order to protect data transmitted among the communicating parties, WEP uses shared secret key of 40 to 140 bits. Following steps are used for implementing the WEP protocol: WEP protocol was designed to provide confidentiality & security for network traffic. Following steps, but not limited to the below, are used for implementing the same:

a. **CRC (Cyclic Redundancy Code):** WEP uses CRC, the most powerful technique, for redundancy checks in data communication. CRC is a method of detecting accidental changes/errors in communication channel. In CRC technique, code is generated using Generator Polynomial & appended to the original frame before transmission and at receiving end message is checked for error using Generator Polynomial, if error free message is decoded for extracting the information and passed on to next higher layer.

b. Confidentiality in the WLAN is implemented through use of cryptographic algorithm, called as RC4 encryption algorithm, known as stream cipher. A stream cipher operates by expanding a short key into infinite pseudo-random key stream. This “key stream” is added as modulo 2 (exclusive-OR-ed) to the data before transmission to produce cipher text. WEP uses “40-bit” encryption that implements a key of length 40 bits and 24 additional bits of system-generated data, 64 bits total. Encryption is done in three phases. First, pseudo-random data sequence of three bytes is generated called as IV – Initialization Vector, to extend the key. Then RC4 algorithm generates key stream based on the new key. Encryption ends with the application of exclusive or function (XOR) between key stream and message thus resulting in encrypted message.

c. The last step is to transmit sequence IV (without encryption) and encrypted message/data in 802.11 frame body field.

The frame/ message after being received to its final destination, the reverse procedure is applied to retrieve the message. Again, the extended key is generated on the basis of transferred IV and shared key; then RC4 algorithm generates key stream. XOR function is applied between key stream and arrived message, and as a result of XOR function, decrypted message is received. The accuracy of received message is checked with CRC sum, if found error free then received message matches the sent one.

**IEEE 802.11(WEP) PROVIDES SECURITY THROUGH, CIA:**

a. Confidentiality is realized by encryption technique, effective means of preventing jeopardizing transmitted data in wireless transmissions. WEP uses the RC4 algorithm developed by RSA Data Security. One of the prime features of WEP is to prevent unauthorized users from gaining access; such purpose is not explicitly set out in 802.11 but is considered an important feature of WEP.

b. Integrity. WEP protocol provides integrity of messages transmitted between stations and access point by using CRC technique, which is part of the encrypted payload of the packet. Integrity of received message is violated when the checksum differentiates. In this case, the message received is rejected.

c. Authentication can be done through an “open system” or “shared key” in either ad-hoc mode or infrastructure mode. A network station or an access point (AP) can grant permission to any station requesting connection in the open authentication system, or only those included in a pre-defined list. In shared-key system, Stations having an appropriate encryption key will be authenticated.

**The security features which are inbuilt in 802.11 are as follows:**

1. **SSID (Service Set Identifier):** SSID is the first security level, to control the wireless network access, provided in 802.11 standards.
The SSID is a unique identifier consisting of sequence of up to 32 characters attribute to the network or a domain. Each wireless client and Access Point belonging to the same network must use the same SSID. Within any network, when a wireless client tries to connect to an AP, the SSID acts as a password, device must share the same to be authorized to join the network. Same is appended to the header of each packet sent over the WLAN and verified by the AP. A client device cannot communicate with an AP unless it is configured with the same SSID.

2) WEP (Wired Equivalent Privacy) Protocol: WEP is a security algorithm introduced as part of 802.11 standards with aiming to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent in a wired medium. It protects authorized users of a wireless LAN from casual eavesdropping. WEP was incorporated in 802.11 to strengthen the security by encrypting data over wireless media while transmission from one point to another. WEP has captured only bottom two layers of the OSI model called data link layer & physical layer, therefore it doesn’t operate end to end security. It uses stream cipher-RC4 for confidentiality and the CRC-32 checksum for integrity.

3) MAC Address Filtering: MAC Filtering is security access control method which enables to access network based on the physical address (MAC Address) of the device. Nodes whose MAC addresses are registered with the access points; they only can be accepted by AP for association and connection; requests sent by other wireless devices will be rejected.

VII. CONCLUSIONS

Wireless made the communication easier in today’s world & has become the dependable technology. From the above discussion, it can be concluded that wireless technology has the advantage over wired technology due to its portability and flexibility, cost effectiveness & ease of use. However, it also has disadvantages also; wireless technologies are prone to interference and noise. But in spite of some disadvantages, wireless is more advantageous and emerging technology. IEEE has developed standard i.e. 802.11 For WLAN and WEP was included for confidentiality & security of the network. However after the usage of WEP, some weaknesses found in WEP, new alternatives such as WPA (based on RC4 and TKIP) and WPA-2 (based on AES/CCMP) have emerged to reduce the lack-of security stigma of wireless networks. As mentioned above, WEP does not provide end-to-end security, but only for the wireless portion of the connection, hence in addition to the above external means like firewall, antivirus etc are also to be considered to strengthen the security to make the full foolproof system. Implementation of the highly secure wireless networks is a very complicated task & required domain expert. Wireless LAN is ever changing technology & very vast area hence timely basis same is to be explored for proper implementation.

Author details

Mr. Sushil Kumar joined Department of Atomic Energy, BARC through OCES-51st Batch of Training School in 2007. Currently he is working as Scientific Officer-E at Heavy Water Board/HWP (M). He completed his B.Tech (E&T) from AKT-University-2007, Post Graduate Diploma (Electronics) with Specialization in Nuclear Energy-2008 from HBNI (BARC), Mumbai & also completed Master of Science (Engineering) by Research in Sensor Development from HBNI-Mumbai. He published few papers in reputed journals. He worked along with TFDS/TPD/TPD division of BARC for the development of H2S Sensors. His area of interest is DSP, Analog & Digital Communication, and Microelectronics & Advanced Instrumentation. He was involved in various projects of DAE, Government of India.

REFERENCES