Analysis the MAC Protocol of IEEE 802.11 Wireless LAN

Md. Mizanur Rahman¹, Farhana Enam²

¹Department of ICE, University of Rajshahi, Bangladesh
²Assistant Professor, Department of ICE, University of Rajshahi, Bangladesh

E-mail: ¹ras5615@gmail.com, ²farhana_ice2008@yahoo.com

ABSTRACT

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to the mobile station. The first, IEEE Standard 802.11a, is an orthogonal frequency domain multiplexing (OFDM) radio in the UNII bands, delivering up to 54 Mbps data rates. The second, IEEE Standard 802.11b is an extension to the DSSS PHY in the 2.4 GHz band, delivering up to 11 Mbps data rates. In this Project study the main emphasis has been given to the MAC layer of the Wireless LAN IEEE 802.11 MAC Protocol. Also the physical layer of the Wireless LAN IEEE 802.11 MAC Protocol has been described. The implementation of the Wireless IEEE 802.11 MAC Protocol is observed through a simulation.

Keywords: WLAN, MAC Protocol, CSMA/CD, MAC Frame Format, IEEE802.11.

1 INTRODUCTION

Wireless networking is a fast-growing technology that allows users to access information and services electronically, regardless of their geographic position without cables. Wireless networks can be classified in two types: Infrastructured Networks and Infrastructureless Networks.

Infrastructure network makes use of a high speed wired or wireless network. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called hand-off.

In ad hoc networks, all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and acquisition operations in inhospitable terrain [1].

2 IEEE802.11 WIRELESS LAN

Early wireless LAN products, introduced in the late 1980s, were marketed as substitutes for traditional wired LANs. A wireless LAN saves the cost of the installation of LAN cabling and eases the task of relocation and other modifications to network structure. However, this motivation for wireless LANs was overtaken by events. First, as awareness of the need for LANs became greater, architects designed new buildings to include extensive rewiring for data applications. Second, with advances in data transmission technology,
there is an increasing reliance on twisted pair cabling for LANs and in particular, Category 3 and Category 5. Thus, the use of a wireless LAN to replace wired LANs has not happened to any great extent.

However, in a number of environments, there is a role for the wireless LAN as an alternative to a wired LAN. Examples include buildings with large open areas, such as a manufacturing plants, stock exchange trading floors, and warehouses; historical buildings with insufficient twisted pair and where drilling holes for new wiring is prohibited; and small offices where installation and maintenance of wired LANs is not economical. In all of these cases, a wireless LAN provides an effective and more attractive alternative. In most of these cases, an organization will also have a wired LAN to support servers and some stationary workstations. For example, a manufacturing facility typically has an office area that is separate from the factory floor but that must be linked to it for networking purposes. Therefore, typically, a wireless LAN will be linked into a wired LAN on the same premises. Thus, this application area is referred to as LAN extension.

Figure 2 indicates a simple wireless LAN configuration that is typical of many environments. There is a backbone wired LAN, such as Ethernet, that supports servers, workstations, and one or more bridges or routers to link with other networks. In addition, there is a control module (CM) that acts as an interface to a wireless LAN. The control module includes either bridge or router functionality to link the wireless LAN to the backbone[2]. It includes some sort of access control logic, such as a polling or token-passing scheme, to regulate the access from the end systems. Note that some of the end systems are standalone devices, such as a workstation or a server. Hubs of other user modules (UMs) that control a number of stations off a wired LAN may also be part of the wireless LAN configuration.

The configuration of Figure 2 can be referred to as a single-cell wireless LAN; all of the wireless end systems are within range of a single control module. Another common configuration, suggested by Figure 3 is a multiple-cell wireless LAN. In this case, there are multiple control modules interconnected by a wired LAN. Each control module supports a number of wireless end systems within its transmission range. For example, with an infrared LAN, transmission is limited to a single room; therefore, one cell is needed for each room in an office building that requires wireless support [3].
2.1 Wireless LAN Requirements

A wireless LAN must meet the same sort of requirements typical of any LAN, including high capacity, ability to cover short distances, full connectivity among attached stations, and broadcast capability. In addition, there are number of requirements specific to the wireless LAN environment. The following are among the most important requirements for wireless LANs.

- **Throughput:** The medium access control protocol should make as efficient use as possible of the wireless medium to maximize capacity.

- **Number of nodes:** Wireless LANs may need to support hundreds of nodes across multiple cells.

- **Connection to backbone LAN:** In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure wireless LANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users and ad hoc wireless networks.

- **Service Area:** A typical coverage area for a wireless LAN has a diameter or 100 to 300m.

- **Battery power consumption:** Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. This suggests that MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station reduce power consumption while not using the network, such as a sleep mode.

- **Transmission robustness and security:** Unless properly designed, a wireless LAN may be interference prone and easily eavesdropped. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.

- **Collocated network operation:** As wireless LANs become more popular, it is quite likely for two or more wireless LANs to operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.

- **License-free operation:** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

- **Handoff/roaming:** The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.

- **Dynamic configuration:** The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion, and relocation of end systems without disruption to other users.

2.2 Wireless LAN Technology

Wireless LANs are generally categorized according to the transmission technique that is used. All current wireless LAN products fall into one of the following categories.

- **Infrared (IR) LANs:** An individual cell of an IR LAN is limited to a single room, because infrared light does not penetrate opaque walls.

- **Spread Spectrum LANs:** This type of LAN makes use of spread spectrum transmission technology. In most cases, these LANs operate in the ISM (Industrial, Scientific, and Medical) bands so that no FCC licensing is required for their use in the United States.

- **Narrowband microwave:** These LANs operate at microwave frequencies but do not use spread spectrum. Some of these products operate at frequencies that require FCC licensing, while others use one of the unlicensed ISM bands [4].
3 MAC PROTOCOL OF IEEE802.11

The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security. We look at each of these in turn.

3.1 Reliable Data Delivery

As with any wireless network, a wireless LAN using IEEE 802.11 physical and MZC layers is subject to considerable unreliability. Noise, interference, and other propagation effects result in the loss of a significant number of frames. Even with error-correction codes, a number of MAC frames may not successfully be received. This situation can be dealt with by reliability mechanisms at a higher layer, such as TCP. However, timers used for retransmission at higher layers are typically on the order of seconds. It is therefore more efficient to deal with errors at the MAC level [5]. For this purpose, IEEE 802.11 includes a frame exchange is treated as an atomic unit, not to be interrupted by a transmission from any other station. If the source does not receive an ACK within a short period of time, either because its data frame was damaged or because the returning ACK was damaged, the source retransmits the frame.

Thus, the basic data transfer mechanism in IEEE 802.11 involves an exchange of two frames. To further enhance reliability, a four-frame exchange maybe used. In this scheme, a source first issues a request to send (RTS). After receiving the CTS, the source transmits the data frame, and the destination responds with an ACK. The RTS alerts all stations that are within reception range of the source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time. Similarly, the CTS alerts all stations that are within reception range of the destination that an exchange is under way. The RTS/CTS portion of the exchange is a required function of the MAC but may be disabled.

3.2 Access Control

The 802.11 working group considered two types of proposals for a MAC algorithm: distributed access protocols, which, like Ethernet, distribute the decision to transmit over all the nodes using a carrier-sense mechanism; and centralized access protocols, which involve regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad hoc network of peer workstations and may also be attractive in other wireless LAN configurations that consist primarily of bursty traffic. A centralized access protocol is natural for configurations sort of base station that attaches to backbone wired LAN; it is especially useful if some of the data is time sensitive or high priority [6].

The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. Figure 4 illustrates the architecture. The lower sub layer of the MAC layer is the distributed coordination function (DCF). DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF. The point coordination function (PCF) is a centralized MAC algorithm used to provide contention function. PCF is built on top of DCF and exploits features of DCF to assure access for its users. Let us consider these two sub layers in turn [8].

3.3 Distributed Coordination Function

The DCF sub layer makes use of a simple CSMA (carrier sense multiple access) algorithm. If station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit; otherwise the station must wait until the current transmission is complete before transmitting. The DCF does not include a collision detection function (i.e., CXSMA/CD) because collision detection is not practical on wireless network. The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

To ensure the smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme. Let us start by considering [7] a single delay known as an interframe space (IFS). In fact, there are three different IFS values, but the algorithm is best explained by initially ignoring this detail. Using an
IFS, the rules for CSMA access are as follows Figure 5.

1) A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.

2) If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.

3) Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.

To ensure that backoff maintains stability, a technique known as binary exponential backoff is used. A station will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled. The binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff time, which helps to smooth out the load. Without such a backoff, the following situation could occur. Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision.

The preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS.

- SIFS (short IFS): The shortest IFS, used for all immediate response actions, as explained in the following discussion.

- PIFS (point coordination function IFS): A midlength IFS, used by the centralized controller in the PCF scheme when issuing polls.

- DIFS (distributed coordination function IFS): The longest IFS, used as a minimum delay for asynchronous frames contending for access.

Figure 6 illustrates the use of these time values. Consider first the SIFS. Any station using SIFS to determine transmission opportunity has, in effect, the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS. The SIFS is used in the following circumstances:

![Fig. 5. IEEE 802.11 Medium Access Control Logic](image_url)
Acknowledgment (ACK): When a station receives a frame addressed only to itself (not multicast or broadcast) it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC protocol data unit (PDU) that requires multiple MAC frames. In this case, the following scenario occurs. A station with a multiframe LLC PDU to transmit sends out the MAC frames one at a time. The recipient acknowledges each frame after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in the sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.

Clear to Send (CTS): A station can ensure that its data frame will get through by first issuing a small Request to Send (RTS) frame. The station to which this frame is addressed should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.

Poll response: This is explained in the following discussion of PCF.

Figure 7 shows the 802.11 frame format. This general format is used for all data and control frames, but not all fields are used in all contexts. The fields are as follows:

<table>
<thead>
<tr>
<th>octets</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>6</th>
<th>2</th>
<th>60 to 2312</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>D/I</td>
<td>Ad</td>
<td>Ad</td>
<td>Add</td>
<td>Add</td>
<td>S</td>
<td>C</td>
<td>Add</td>
<td>Frame</td>
</tr>
</tbody>
</table>

FC= Frame control  
D/I= Duration/Connection ID  
SC= Sequence control

Frame control: Indicates the type of frame and provides control information, as explained presently.

Duration/connection ID: If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.

Addresses: The number and meaning of the address fields depend on context. Address types include source, destination, transmitting station, and receiving.

Sequence control: Contains a 4-bit fragment number subfield, used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.

Frame body: Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
• Frame check sequence: A 32-bit cyclic redundancy check.

The frame control field, shown in Figure 6.4b, consists of the following fields:

• Protocol version: 02.11 version, currently version 0.
• Type: Identifies the frame as control, management, or data.
• Subtype: Further identifies the function of frame. The 14.3 Defines the valid combinations of type and subtype.
• To DS: The MAC coordination sets this bit to 1 in a frame destined to the distribution system.
• From DS: The MAC coordination sets this bit to 1 in a frame leaving the distribution system.
• More fragments: Set to 1 if more fragments follow this one.
• Retry: Set to 1 if this is a retransmitting station is in a sleep mode.
• Power management: Set to if the transmission station is in a sleep mode.
• More data: Indicates that a station has additional data to send. Each block of data may be sent as one frame or a group of fragments in multiple frames.
• WEP: Set to if the optional wired equivalent protocol is implemented. WEP is used in the exchange of encryption keys for secure data exchange.
• Order: Set to 1 any data frame sent using the Strictly Ordered service, which tells the receiving station that frames must be processed in order [9].

3.4 Various MAC frame types

3.4.1 Control Frames

Control frames assist in the reliable delivery of data frames. There are six control frame sub types:

• Power save-poll (PS-Poll): This frame is sent by any station to the station that includes the AP (access point). Its purpose is to request that the AP transmit a frame that has been buffered for this station while the station was in power-saving mode.
• Request to send (RTS): The station sending this message is alerting a potential destination, and all other stations within reception range, that it intends to send a data frame to that destination.
• Clear to send (CTS): This is the second frame in the four-way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
• Acknowledgment: Provides an acknowledgment from the destination to the source that the immediately preceding data, management, PS-Poll frame was receive correctly.
• Contention-free (CF)-end: Announces the end of a contention-free period that is part of the point coordination function.
• CF-end+CF-ack: Acknowledges the CF-end. This frame ends the contention-free period and releases from the restrictions associated with that period.

3.4.2 Data Frames

There are eight data frame subtypes, organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames are as follow:

• Data: This is the simplest data frame. It may be used in both a contention period and a contention-free period.
• Data + CF-Ack: May only be sent during a contention-free period. In addition to carrying data, this frame acknowledges previously received data.
• Data + CF-Poll: Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
• Data + CF-Ack + CF-Poll: Combined the functions of the Data + CF-Ack and CF-Poll into a single frame.
3.4.3 Management Frames

Management frames are used to manage communications between stations and APs. The following subtypes are included:

- Association request: Sent by a station to an AP to request an association with this BSS. This frame includes capability information, such as whether encryption is to be used and whether this station is pollable.
- Association response: Returned by the AP to the station to indicate whether it is accepting this association request.
- Reassociation request: Sent by a station when it moves from one BSS to another and needs to make an association with the AP in the new BSS. The station uses reassociation rather than simply association so that the new AP knows to negotiate with the old AP for the forwarding of data frames.
- Reassociation response: Returned by the AP to the station to indicate whether it is accepting this reassociation request.
- Probe request: Used by a station to obtain information from another station or AP. The frame is used to locate an IEEE 802.11 BSS.
- Probe response: Response to a probe request.
- Beacon: Transmitted periodically to allow mobile stations to locate and identify a BSS.
- Announcement traffic indication message: Sent by a mobile station to alert other mobile stations that may have been in low power mode that this station has frames buffered and waiting to be delivered to the station addressed in this frame.
- Dissociation: Used by a station to terminate an association.
- Authentication: Multiple authentication frames are used in an exchange to authenticate one station another, as described subsequently.
- Deauthentication: Sent by a station to another or AP to indicate that it is terminating secure communications [10].

4 SIMULATION RESULT

Figures should be labeled with A Simulation Environment created using the programming language Matlab-7 was studied to observe the IEEE 802.11 MAC protocol implementation. Various parameters of an ad hoc network employing IEEE-802.11 protocol such as number of mobile nodes, their data transmission range, node mobility, data transmission duration was varied to find out the performance of the MAC protocol.

In this simulation the data packet transmission between various nodes has been shown through solid red line and the acknowledgement data transmission is shown using solid green lines as shown in the following Figure:

![Data and ACK packet transmission between source and destination](image-url)

Fig. 8. Data and ACK packet transmission between source and destination

And also the RTS and CTS data transmission are also shown through dotted red and green lines respectively, which is shown below:
Fig. 9. Data, ACK, RTS and CTS packet transmission between source and destination

5 CONCLUSION

Through study and also simulation it is found that the IEEE 802.11 standard quite efficiently overcomes the collisions of control packets. It can also reduce the hidden terminal problem and it can also handle the exposed terminals problems to some extent.

From the Ad hoc network simulation study it is found that IEEE 802.11 MAC Protocol can quite efficiently establish Wireless communication link among various nodes when the number of nodes transmission range, nodes mobility, data transmission duration are varied.

The goals of the IEEE 802.11 standard is to describe a WLAN that delivers services previously found only in wired networks, e.g., high throughput, highly reliable data delivery, and continuous network connections. In addition, IEEE 802.11 describes a WLAN that allows transparent mobility and built-in power saving operations to the network user.

6 REFERENCE