Umeå University, Sweden
Department of Computing Science

Master Thesis

MAC Algorithms in Wireless Networks

Applications, Issues and Comparisons

Shoaib Tariq

Supervisor: Dr. Jerry Eriksson
Examiner: Dr. Per Lindström

Dedicated to
My Loving
Parents

ABSTRACT

This thesis report seeks to study and analyze in-depth regarding various medium access control (MAC) layer algorithms and protocols that have been implemented and proposed for wireless networks. Theory begins with a short overview of basic MAC algorithms used in wired networks as well as some problems appear when these algorithms used for wireless medium access control layer. Then special MAC algorithms for world of wireless are discussed according to the particular type of wireless networks like wireless local area network (WLAN), wireless personal area network (WPAN), wireless sensor network (WSN) and wireless cellular networks. A detailed description of these algorithms and protocols together with their issues and comparison is given within each type of network. Finally, the comparison of different forms of wireless network systems with respect to the MAC algorithms belong to them is presented.

CONTENTS

1 INTRODUCTION

The world of today has become quite fast and reliable mainly because of the wireless communication.

1.1 Wireless Communication

Wireless communication is the transfer of data from one place to another through electromagnetic waves. It is a mode of communication that uses free space instead of wires. Hence the data travels in the air as same as light does. Wireless communication mostly related to radio, microwave and infrared waves.

Importance: This type of communication is quite swift with a better output. Data can be exchanged in less time. People far away from each other can easily communicate at any time e.g., use of online chatting, cell phones, e-mails etc. It has many other advantages like to install the wireless system in a building will be easy comparative to fix all wires in the building for the wired network would be time taking, complicated and also headache.

1.2 Wireless Network

The system that enables wireless data communication is called the wireless network, e.g., radio channel network, TV network etc. It consists of either computers, laptops, notebooks, routers, switches, cell phones, portable phones, PDA's, related operating systems / softwares, access points (AP), base stations (BS), antennas or towers etc.

One network can interconnect with other network or sub network. As WLAN is one network but it can interconnects Bluetooth wireless system or can also support the wireless ad-hoc network. Furthermore, 2G and 3G cellular networks are running together, and they are adaptive to each other as well.

Types of Wireless Networks

There are various types of wireless networks being used as; infrastructure-based WLAN, wireless Ad-hoc network, wireless personal area network (WPAN), wireless cellular network, satellite system, television network and wireless sensor network (WSN) etc.

Each type of network uses slightly different techniques and algorithms from each other in all aspects including *MAC algorithms* as well. MAC plays vital role in wireless communication. It will be exposed comprehensively in the coming section 2; such that why it is needed, its mechanism / technique, some basic MACs and the reasons of specialized MAC for wireless domain as compared to the wired network.

2 Medium Access Control

How to transfer the data safely when there is more than one user accessing a single channel simultaneously ?

Medium Access Control (MAC) algorithms are used to allow several users simultaneously to share a common medium of communication in order to gain maximum of channel utilization with minimum of interference and collisions. MAC is similar to traffic regulations in the highway. Several vehicles cross the same road at a time but rules required to avoid collision e.g., follow the traffic lights, building the flyovers etc. [1].

MAC belongs to layer 2; the Data Link Control layer (DLC) of the ISO *OSI reference model*. Layer 2 is subdivided into the MAC layer 2a, and logical link control (LLC) layer 2b. The task of DLC is to establish a reliable point-to-point or point–to-multipoint connection between different devices over wired or wireless medium.

2.1 Basic MAC Algorithms

Many MAC algorithms and protocols have been successfully used in wired networks for a long time. Some of them are quite famous and elegant algorithms such as ALOHA and *Carrier Sense Multiple Access* (CSMA). These are very basic schemes for multiple access channels, and they are also the basis for wireless channel allocation schemes. Therefore, we shall review them briefly in the following to develop better concepts for wireless MAC algorithms.

i. ALOHA

In 1970s Norman Abramson proposed a new and reliable algorithm to solve the channel allocation problem in wired network. Abramson worked with his colleagues at the University of Hawaii to develop this method called ALOHA or Pure ALOHA. Its another version is called Slotted ALOHA [3].

Pure ALOHA is a random access protocol. A user can access the channel whenever it has data to be transmitted. Definitely, there will be a collision. However, after transmission the user waits for an acknowledgment from separate feedback channel. If there is collision, the sender waits for a random amount of time and retransmits the data. Pure ALOHA does not relate to time synchronization.

Slotted ALOHA divides the time into equal time slots of length greater than the packet duration. Each user has synchronized clock and transmits the data only at the beginning of new time slot. This helps in a discrete distribution of accessing the channel. But collision is not prevented absolutely; there is a collision with portions of data packets.

ii. CSMA

ALOHA does not listen to the channel before transmission. On the other hand, *carrier sense multiple access* (CSMA) algorithm is based on the concept that each station on the network is able to sense the channel before transmitting the data packet. Sensing the channel means to monitor the status of channel whether it is idle or busy. If the channel is idle/free, then station can transmit the data. But if the channel is sensed busy, the station will wait and keep on sensing the carrier till it becomes free. This method decreases the probability of collision.

There are several versions of CSMA exist:

- **non-persistent**: In this type of CSMA, a station senses the channel first. If the channel is free then it starts transmission immediately. But if channel is busy then the station does not continuously sense the channel, rather it waits for a random amount of time and then repeats the algorithm [1].
- **p-persistent**: It is applied to slotted channel. Here stations also sense the medium. If the medium is free, a station transmits the packet with a probability of *p*, or with probability of *1-p* if the station defers to next slot.
- **1-persistent**: When a station wants to send the data, it first senses to the channel whether it is free or busy at the moment. If it is busy, the station waits until it becomes free. And if the station detects an idle channel, it transmits a data frame. When the channel becomes free the two or more neighboring stations can transmit data at the same time. This will cause collisions. If the collision occurs, the station waits a random amount of time and repeats the method. The algorithm is called 1-persistent because the station transmits with a probably of 1 whenever it finds an idle channel.

2.2 Back-off Algorithms

Thus, collision and loss of packets are the major problems in wireless networks compared to wired networks. Then how much time should be spent for waiting when the carrier is busy, waiting after collision or loss of packets etc. are other critical issues in wireless domain. However, some techniques and methods have also been applied besides the MAC algorithms to overcome these issues. The terminologies like *random amount of time / random back-off time* have been mentioned in ALOHA, CSMA and will be used in subsequent protocols too. The purpose of these techniques is to make a transparent and justified way of accessing the wireless medium. The real algorithms producing the random amount of time are the *Back-off Algorithms*. There are two types of such algorithms;

i. Random Back-off time / Binary Exponential Back-off

This is the mostly used algorithm in order to select the random amount for the duration of waiting time in the network. Here the random amount of time is the random back-off time that counts downwards to zero. This time delays the access of medium in order to provide transparent and collision free environment for all nodes in the network. Whenever, if any node finds the medium busy in the network, it is supposed to get a random value within a **contention window** for back-off time. The node starts counting down its back-off time only when the medium becomes free. Each node may have different or same amount of time but within contention window. This random waiting time avoids collisions; otherwise all nodes would have accessed the idle medium at the same time. After finishing that random time, they start sensing the medium. As soon as a node senses the channel is busy, it loses this turn and it will select another back-off time for the next cycle. On the other hand, if a node gets the medium free after waiting for random time, it can access the medium immediately [1].

Contention window (CW) is set with an initial size e.g. $CW_{\min} = 7$. The back-off time is selected from the CW and it could be any value between 1 and 7. CW becomes double + 1 at each time for every collision or lost frame. The window can take on the values 7, 15, 31, 63, 127, 255 and so on. Let maximum size of CW in this example is $CW_{\max} = 255$. The collision indicates the load on the network, and then doubling the value of CW can minimize the chances of collision. It is hard to select the same random back-off time using large CW. This algorithm is also called the *Binary Exponential Back-off* (**BEB**), because CW doubles (having linear graph) at each time of collision [1]. The value of CW is reset to its original minimum value (CW=7) as soon as any transmission completes successfully after the occurrence of collision. The standard size of CW in **802.11a**: $CW_{\min} = 15$ $CW_{\max} = 1023$, and in **802.11b**: $CW_{\min} = 31$ $CW_{\max} = 1023$.

ii. MILD

The MILD stands for *multiplicative increase and linear decrease*. The contention window (CW) is also set in this algorithm. Initially a minimum value is selected for CW, say CW = 5. At each time of collision, instead of doubling the CW, here the CW is increased by multiplicative factor; say 1.5. Thus, CW would become 5x1.5 = 7.5, at first collision. Moreover, at the time of successful transmission after collision the CW is linearly decreased; let's assume by 1. So, it would be 7.5 – 1 = 6.5 [5].

2.3 Specialized MAC in Wireless

The main question is why elaborated schemes used in wired network are fail in wireless world. This is due to several effects that occur only in wireless network. To explain in detail, let us consider first **Carrier Sense Multiple Access with Collision Detection** (CSMA/CD), one of the MAC schemes being used in wired networks.

CSMA/CD works as follows: A sender A wants to transmit data to a receiver B. Then A senses the medium (wire or coaxial cable) to check that the medium is free or not. If it is busy, the A waits until it becomes free. But if the medium is free, the A starts transmitting data and continues to listen into the medium. If sender A detects a collision while sending data, it stops at once and sends a jamming signal [2].

CSMA/CD aims that the signal should reach the receiver without collisions. The sender is the one detecting collisions. This is not a problem using wire, as more or less the signal strength remains same all over it. If collision occurs somewhere in the wire, everybody notices that. It is not the case that a sender listens into the medium only to detect the collision at its own location, rather in reality is trying to detect a possible collision at the receiver side [1]. Why does this scheme fail on wireless networks?

The situation is different in wireless networks. As there are no wires and the signal propagates in more than one direction and faces resistance from walls, trees and other things etc. This implies, "*the strength of a signal decreases proportionally to the square of the distance to the sender"*. Let's apply CSMA/CD here. The sender senses the medium and finds it idle. It starts sending but a collision occurs at the receiver due to the second sender. It is because of hidden terminal problem [1]. Collision detection is very difficult in wireless scenarios as there is no physical connection between stations. Also the transmission and detection range is limited, and thus data transmissions of various stations cannot be detected every time. All critical problems which are the reasons for special MACs required in wireless networks explained below:

i. Hidden Terminal Problem

Consider the situation as shown in the Figure 2.1. There are three mobile phones A, B and C. The transmission and detection range of A reaches B, but not C. The same applies to C. The transmission and detection range of C reaches B, but not A. Hence A cannot detect C and C cannot A either. That means A is ***hidden*** for C and vice versa. The transmission range of B reaches both A and C.

A starts sending to B, C does not receive this transmission. At the same time C also wants to send something to B and senses the medium. The medium appears to be free, thus the carrier sense fails. C now starts sending and causes a collision at B. The both senders A and C cannot detect this collision at B and will keep on sending. Also, both will assume that the data has been transmitted without errors, but actually the collision has destroyed the data at the receiver. This is only due to hidden problem as A and C both are hidden to each other.

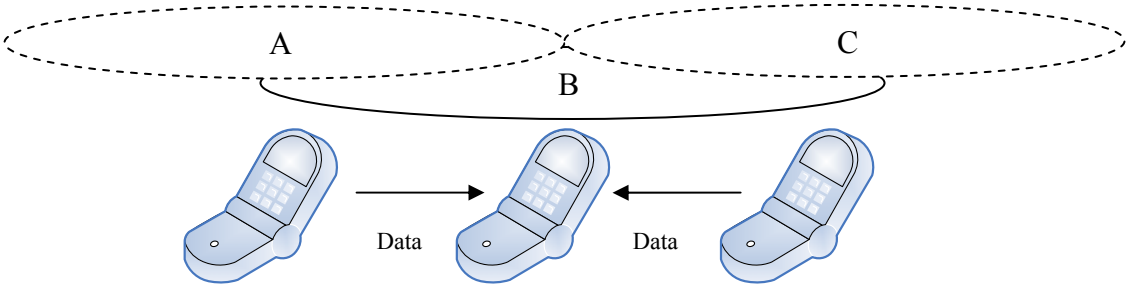


Figure 2.1: Collision at B due to Hidden Terminal Problem

ii. Exposed Terminal Problem

This effect does not destroy data, but causes only unnecessary delays. Consider the same scenario shown in Figure 2.1. Now B sends something to A. Simultaneously C wants to transmit data to some other mobile phone outside the interference ranges of A and B. C senses the carrier and detects that the carrier is busy just because of B's signal. It will postpone its transmission until it detects the medium becomes idle. But A is outside the range of C, so waiting is not required. The collision that would have occurred at B does not matter, because it is too weak to propagate to A. So C is exposed to B.

iii. Near Terminal

The situation in Figure 2.2 shows three mobile phones, where A and B are both sending to C with the same transmission power. Consider C as a base station (BS). As the strength of a signal decreases proportionally to the square of the distance, B's signal drowns out A's signal because B is near to BS. As a result, C cannot receive A's transmission [1].

iv. Far Terminal

Now C has to send signals to both terminals A and B. As B is quite near to BS, it will receive the transmission clearly. But A is far enough from C that it would not be able to get fair transmission. Hence stations that far away are badly affected by the near terminals and other resistance like free space loss, reflection etc.

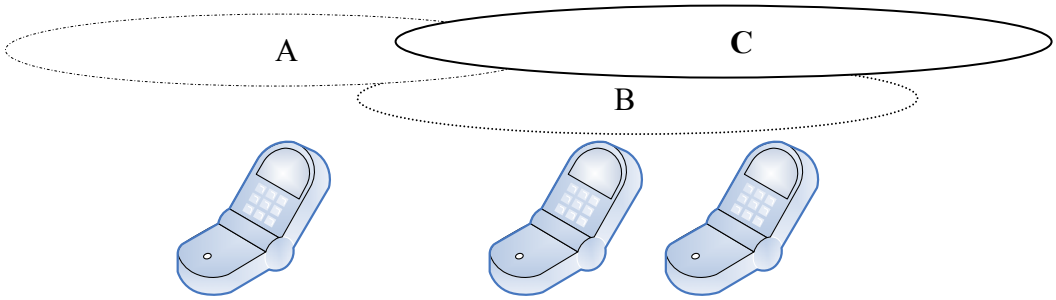


Figure 2.2: Near and Far Terminals

In the following, various MAC algorithms and protocols that have been implemented and proposed in different forms of wireless network will be analyzed with their issues and comparison with each other. Starting with MAC in WLAN then followed by WPAN, WSN and cellular.

3 Wireless Local Area Network

Wireless local area network (WLAN) is a fast-growing market in wireless domain. WLAN covers a limited geographical area as it is restricted within buildings, a campus or in a room etc. It can be divided into two groups according to their network configurations. First type of WLAN is infrastructure-based wireless network, and second is the infrastructure-less wireless network usually called *ad hoc* wireless network.

3.1 Infrastructure-based WLAN

In Infrastructure-based networks, communication can take place only between an access point (AP) and the wireless terminals. There is no direct communication between wireless terminals; usually called nodes or stations. AP does not control just wireless medium, but it also acts as a bridge to other wireless or wired networks.

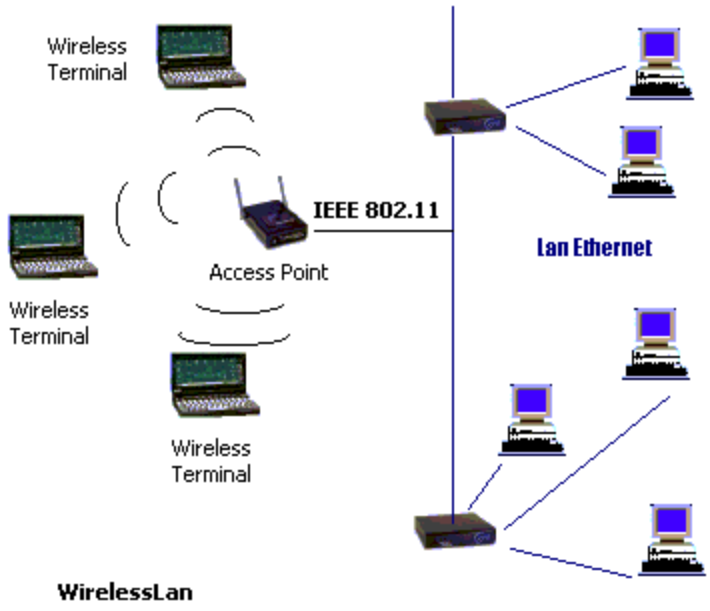


Figure 3.1: Infrastructure-based WLAN having AP communicating with Wireless terminals and with wired LAN

This type of network uses many medium access schemes. These schemes mostly based on carrier sensing and virtual sensing, trying to reduce collisions, provide fair medium access by using back-off algorithms and avoiding hidden and exposed terminal problems.

3.1.1 MAC Algorithms in Infrastructure-based WLAN

Variety of medium access methods and techniques has been designed for WLAN. Many of them have been deployed successfully. New methods are still being proposed in the market. The paper is going to narrate some of the MAC methods which have been implemented successfully for the commercial use.

i. CSMA/CA

The basic CSMA scheme has come up with the concept of *collision avoidance* by using *random back-off time*. So, the CSMA/CA introduces the BEB algorithm in order to create some fairness for waiting time and importantly to reduce the probability of collisions. In the very first cycle, if a station finds the channel free starts its transmission immediately. Consider the scenario in Figure 3.2, the station B gets free medium in first cycle and hence starts transmission. All other stations A, C and D got the busy channel in first cycle, they now select the random back-off time each within a contention window (CW). In the beginning of next cycle, the stations A, C and D want to send data and start sensing the medium. As soon as stations sense the idle medium, they begin to counting their back-off times. The station D had small back-off time, D finishes it very early and gets the free medium and thus starts transmission. But other two stations A and C continued with back-off time, and after finishing their times they got a busy medium. Now A and C will wait for next cycle having new back-off time and repeat the whole algorithm again. Moreover, if two stations finish their back-off times simultaneously, they will start their transmission together provided the medium is idle, and hence there will be a collision. The collision triggers a new value of contention window (double+1). As soon as the receiver gets the packet and it answers with an acknowledgment packet ACK. The ACK confirms the correct reception of data. If no ACK is received by sender, it will retransmit the packet in future. But the sender has to follow the whole algorithm again to access the channel. No special rule has been designed yet for retransmission.

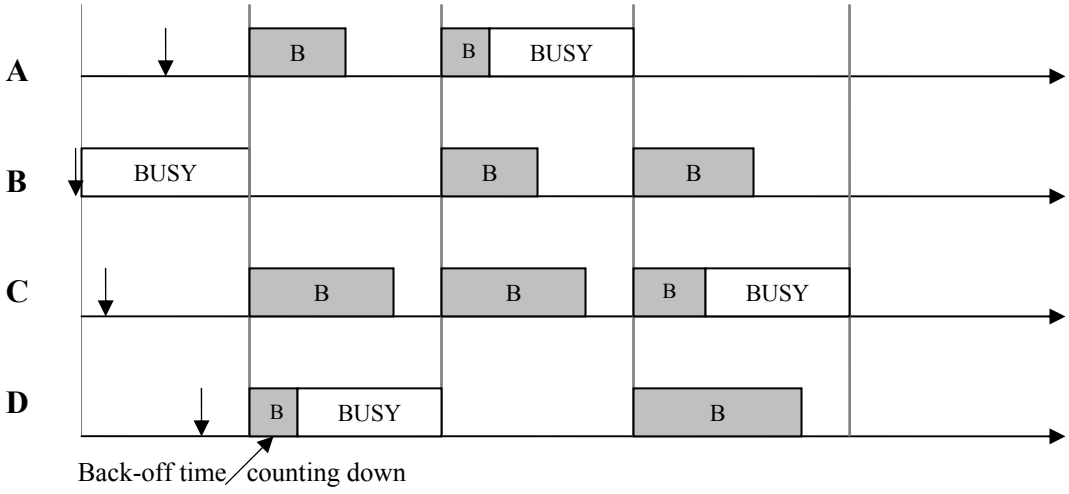


Figure 3.2: Stations accessing the medium using CSMA/CA

Issues: The back-off algorithm in CSMA/CA just tries to avoid collisions, but could not remove it all. Depending on the size of the CW, values of random back-off time either so small that causing many collisions or values may be quite big causing unnecessary delay. Furthermore, there is unfairness in waiting for back-off time. The nodes waiting their whole back-off time and then find the channel is busy, they will select new time for the next cycle which is severe injustice. They are not given any extra credit of previously waiting time. Secondly, CSMA/CA has failed to solve the hidden and exposed terminal problems. In wireless network it is obvious that some stations are out of the transmission and detection range of each other. It is possible that transmission and detection range of A is reaching to B, but not to C. Same is the case with the C. That means A and C are hidden to each other. Therefore, when A gets the medium free and transmits data to B, the C cannot detect that the medium is busy and it can also transmit data to B at the same time. Hence, there will be a collision. The exposed terminal problem also exists here as we have already discussed these problems in section 2.3.

ii. MACA

In order to overcome the hidden and exposed terminal problems in CSMA/CA, the new technique *multiple access with collision avoidance* (MACA) was introduced in many MAC layer protocols of WLAN. It uses two additional packets Request-to-Send (RTS) and Clear-to-Send (CTS). The RTS/CTS are the control packets exchanged between two nodes just before the transmission of actual data. The binary exponential back-off (BEB) algorithm is also applied to provide fairness while accessing the medium.

When a sender wants to send the data and finds the medium free, it first sends an RTS packet to the receiver (after waiting for back-off time if the medium was found busy in previous cycle). RTS indicates that sender wants to send a data. The RTS packet is not given any higher priority as compared to other data packets. It possesses the size of data indicating the duration of whole data transmission. After receiving the RTS, the receiver responds with the CTS packet, provided that the receiver is willing to accept the data at the moment. Otherwise CTS is not responded to the sender. The CTS packet gives the permission to the sender that it can transmit data to the intended receiver. Now the sender transmits the actual data safely to the required receiver. The CTS packet also contains the length of data transmission. All other stations hearing RTS or CTS come to know that particular stations are busy and hence they avoid interfere that transmission. Any node overhears an RTS packet it defers its transmission until corresponding CTS packet is expected to be received. A node overhearing a CTS packet defers its transmission till the end of corresponding data transmission. All these steps are clearly shown in the Figure 3.3. Thus, the mechanism relieves the problem of hidden and exposed terminals by successfully exchange of RTS-CTS-DATA packets. There is no acknowledgment packet (ACK) in MACA scheme.

After transmitting the RTS packet, if sender does not receive the CTS packet within a designated period, it is assumed a collision and eventually will time out. The packet is scheduled for retransmission in the future.

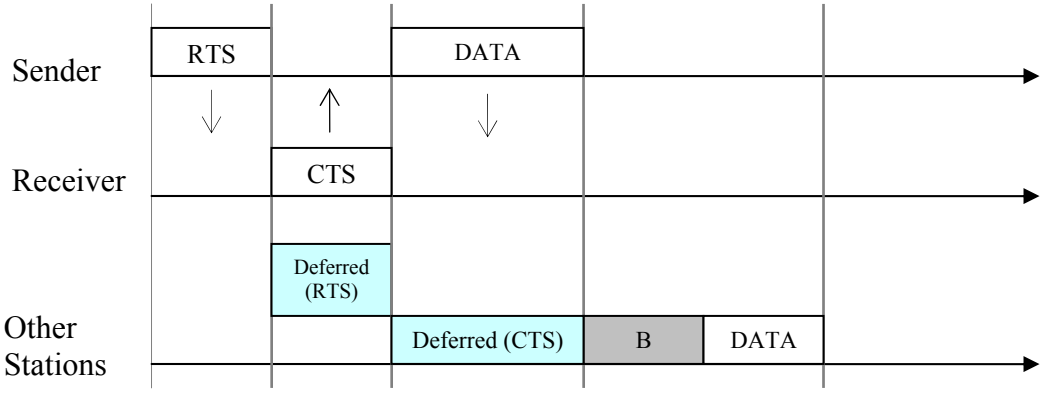


Figure 3.3: Stations accessing the medium using MACA

Issues: There is a use of extra packets RTS/CTS, which are overhead and load in the network. They are likely to cause delay in communication. Moreover, the scheme does not completely eliminate the problem of hidden and exposed terminal exists in CSMA/CA. The two RTS packets can collide themselves transmitted simultaneously by two adjacent nodes. CTS packet can also collide with the RTS of the neighbor.

iii. MACAW

The improved and modified version of MACA was renamed as *MACA for Wireless* (MACAW). It follows basically the same RTS/CTS scheme of MACA.

The first improvement is the addition of acknowledgment (ACK) packet after each successful data frame. It improves the reliability as well as system throughput. Secondly, it uses *multiplicative increase and linear decrease* (MILD) as a back-off algorithm instead of BEB. Another different approach of MACAW is an additional Data-Sending (DS) packet to be sent by a node before transmission of actual DATA packet. The DS packet informs the overhearing stations that RTS-CTS exchange has been successful and data transmission is about to begin. The overhearing stations defer all their transmissions till the Data and ACK packets have to be exchanged. Figure 3.4 is a model of MACAW method. Besides all, it also adds the Request-for-Request-to-Send (RRTS) packet. A node receiving the RTS packet may not be able to reply with its CTS packet if it is busy with another transmission. That increases the back-off counter of the sender. To avoid the problem if a receiver of RTS cannot reply with CTS packet immediately (being busy with another transmission), it transmits RRTS packet to the sender as soon as it becomes free. As a result, sender will transmit RTS packet as early as possible [5]. Hence, RTS-CTS-DATA-ACK packets exchanged while transmission of data with help of DS and RRTS packets as well. MACAW improves the throughput and fairness in WLAN.

Issues: It has same issues of using control packets RTS/CTS with now even more packets of ACK, DS and RRTS are used in the network that increase the overhead and the load of traffic. And, the problem of collision between these packets still exists. Furthermore, MACAW does not distinguish between different priority classes. All nodes

have equal right to access the channel and there is no distinction among different types of traffic.

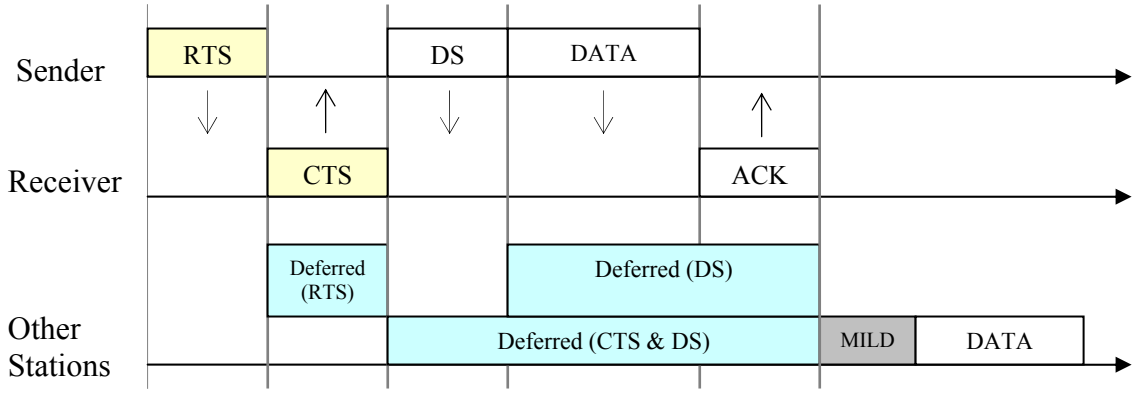


Figure 3.4: Stations accessing the medium using MACAW

iv. IEEE 802.11 MAC

The IEEE works here as well by introducing IEEE standard 802.11 for WLAN. The standard's number indicating that it belongs to the group of 802.x LAN standards, e.g., 802.3 for Ethernet and 802.5 for Token Ring etc. Therefore, this standard IEEE 802.11 focuses only on physical (PHY) and medium access control (MAC) layers. Basically MAC layer provides the mandatory asynchronous data service and an optional time-bounded service. The 802.11 MAC offers both types of services for infrastructure-based WLAN, while it offers only asynchronous data service for ad-hoc network mode.

The three different access mechanisms have been defined for IEEE 802.11 MAC; first one is based on CSMA/CA, second is on MACA/MACAW, and the last one is the Polling method. The first two methods can also be categorized as *distributed coordination function* (DCF), it offers only asynchronous data service. The third method can be called *point coordination function* (PCF) and it offers both asynchronous and time-bounded service. The IEEE 802.11 MAC schemes are also called *distributed foundation wireless medium access control* (DFWMAC) [1].

The unique feature of 802.11 MAC is the fix parameters for waiting time before accessing the medium. This waiting time is other than the back-off time. There are three different types of parameters. They define the priorities of medium access.

- **DCF inter-frame spacing (DIFS)**: Any node in the network if finds the medium free for the transmission, it has to wait first for duration of DIFS. This parameter has longest waiting time and has lowest priority of medium access.
- **Short inter-frame spacing (SIFS)**: It is the shortest waiting time for medium access, and used before sending the ACK or polling responses. It has highest priority being shortest waiting time.
- **PCF inter-frame spacing (PIFS)**: This waiting time is used in polling method. An access point has to wait PIFS before accessing the medium. This waiting time is between DIFS and SIFS, and obviously has medium priority [1].

a) DFWMAC with CSMA/CA

This standard is based on CSMA/CA using BEB algorithm. The major enhancement is the inclusion of *DIFS* and *SIFS*. Every time when a node finds the medium idle, then it has to wait for the time of DIFS. This technique is for every node acting part in that network. After DIFS, a node starts its back-off time (if the medium was busy in last cycle), and then it can transmit data if the medium is still free, as node B starts first in the Figure 3.5. Other nodes will wait for the next cycle. There is also a time of SIFS for receiving nodes. After receiving the required packet a receiver waits for SIFS and then replies with ACK packet given in Figure 3.6.

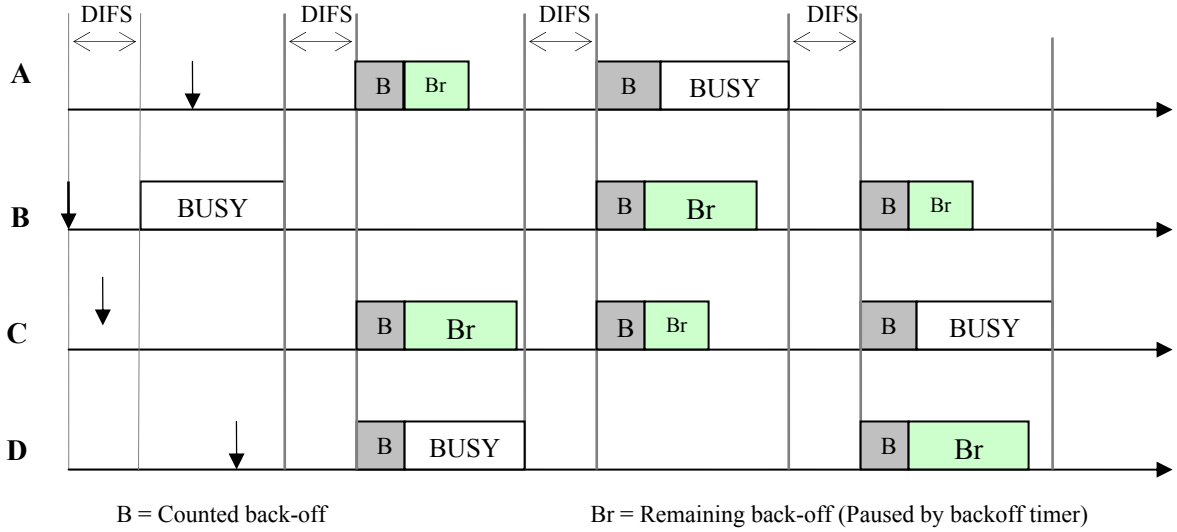


Figure 3.5: Stations accessing the medium using IEEE 802.11 MAC

IEEE 802.11 (DFWMAC) introduces another vital feature by adding *back-off timer* in the random back-off time algorithm. A node finishes its back-off time very first and finds the medium free, it will start its transmission. But other nodes having longer back-off time would not continue to count down, rather they pause their back-off timer (Br) and will wait for next cycle as nodes A and C did in second cycle shown in the Figure 3.5. After getting the channel idle and wait for DIFS, the nodes will resume their paused back-off time. This implies that the deferred stations are not supposed to choose back-off time again but to carry on with the same value until it finishes. Hence the scheme provides a great deal of fairness and improvement for accessing the medium. But the renowned hidden and exposed terminal problems exist here too.

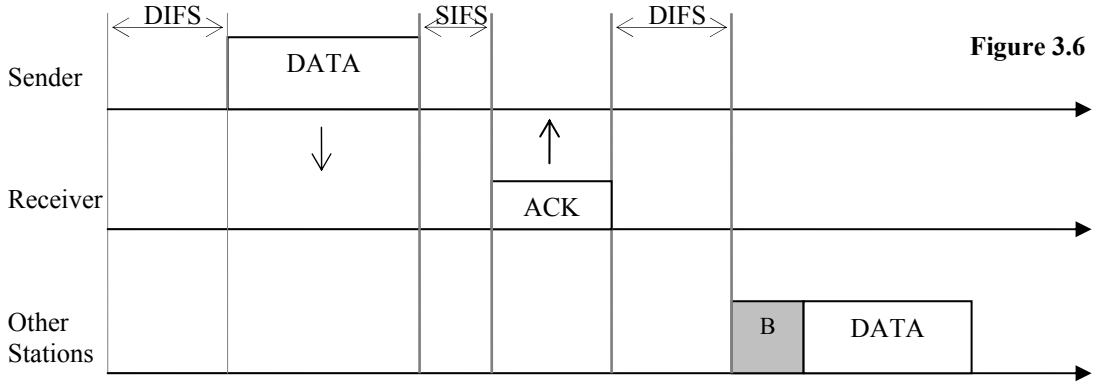


Figure 3.6

b) DFWMAC with RTS/CTS

To overcome the hidden and exposed terminal problems, the 802.11 MAC introduces RTS/CTS control packets which belong to MACA. The algorithm has same functionality of *DFWMAC with CSMA/CA* but with the extension of RTS/CTS and network allocation vector (NAV).

Consider the Figure 3.7, a sender X finding the medium free then it waits for DIFS. Now if the medium is still free then it will transmit request-to-send (RTS) packet to the desired station. RTS packet contains the receiver address and duration of whole data transmission. As the required receiver Y receives the RTS comes to know about the upcoming transmission. If Y is ready to accept the data then it will wait for SIFS and send a CTS packet to X. Any station overhears an RTS or CTS packet, will set the NAV to defer itself from medium access until the end of data transmission and corresponding ACK frame received by sender. NAV is the virtual sensing as it reserves the medium exclusively for one transmission. It also specifies the point at which deferred stations can try to access the medium again. In this way the scheme has tried successfully to avoid hidden problem, but exposed terminal problem emerges more.

After receiving the CTS from Y, the sender X will send the data after waiting for SIFS. The receiver Y will wait for SIFS after receiving the data and then reply with ACK packet. The transmission has been completed and NAV also lets the medium free to start the standard cycle again.

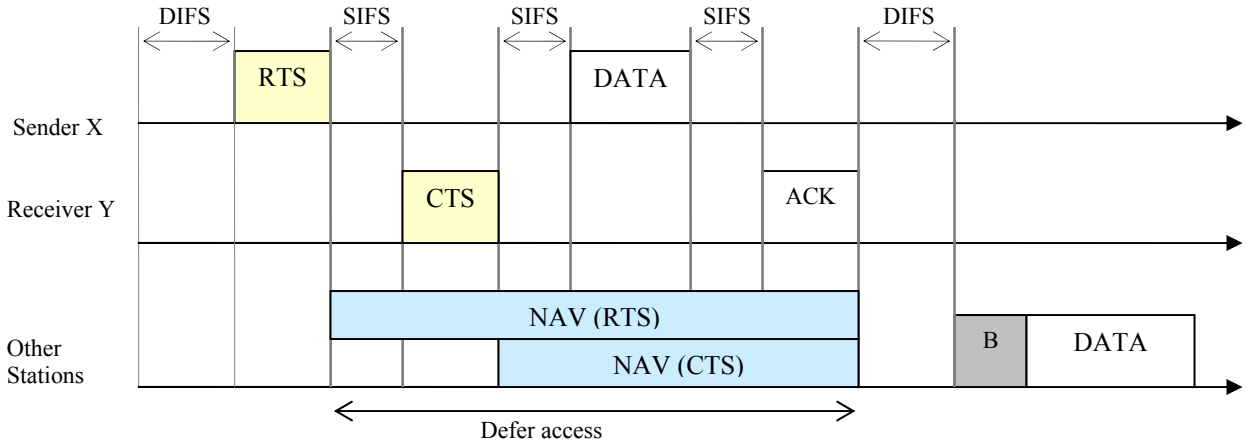


Figure 3.7: IEEE 802.11 with RTS/CTS extension

c) DFWMAC with Polling

The polling is the entirely different approach for medium access control as compared to the previous discussed schemes. It offers time-bounded service as well besides asynchronous data service and thus it is using point coordination function (PCF) mechanism instead of DCF. The concept of PCF is that it requires an access point (AP) that controls the medium access and polling of the stations in the network.

Polling is the technique that all the stations communicate through an AP. They do not contact directly with each other rather AP allows each station one by one to send the data. AP is like master and all other stations are its slave. AP has a list of stations used for polling. The list is based on some priority like round robin, randomly or reservation etc., [1]. The point co-ordinator in the AP divides the access time into a contention period and a contention-free period. The contention period is used for first two MAC schemes of IEEE 802.11 using DCF approach.

Polling starts only in contention-free period. When the AP finds the medium idle, then it has to wait for PIFS before accessing the medium. As PIFS is smaller than DIFS than no other station can access earlier. After waiting for PIFS, AP sends the D1 to first station as a downlink. This station sends data U1 an uplink after waiting SIFS. Now, the AP waits SIFS this time and sends D2 to second station. This station may answer with data U2 to the AP (see in Figure 3.8). The polling continues in the same way with other stations in the list. The AP will poll all stations in the list, even the stations do not want to send data will also be polled; as it happens with station 3 in the Figure 3.8. When the contention-free period ends, the point coordinator issues an ending flag (CF_{end}).

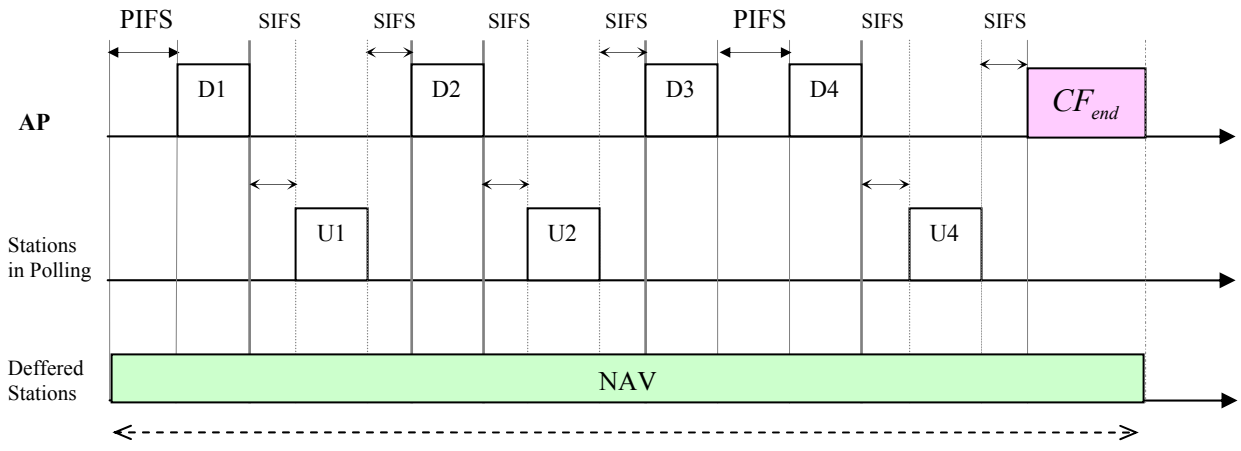


Figure 3.8: Contention-free period access using Polling mechanism

Issues in DFWMAC (802.11 MACs):

The first basic method has only the renowned hidden and exposed terminal problems as it is using CSMA/CA. Although the back-off timer has been introduced but it is possible that two or more stations have same back-off time values and definitely they will access the medium at same time. The back-off time is not for the purpose to solve hidden and exposed terminal problem, rather it is providing the fairness among several stations to access the medium.

To overcome the problems exist in the first method, the DFWMAC was modified by adding RTS/CTS control packets and NAV virtual sensing. RTS/CTS packets avoid hidden and exposed terminal problems just in case when RTS/CTS are exchanged safely. It is possible that two or more neighboring nodes may transmit RTS at the same time, and that results in collisions. Moreover, RTS/CTS packets cause delay in communication and also they consume extra bandwidth. Using NAV is also solving the hidden terminal problem in great manner. But exposed terminal problem is appearing more significantly because all stations overhearing RTS/CTS of stations X and Y set their respective NAV. The station who wants to send data to station Z, it will unnecessarily defer its access to the medium.

As for as polling is concerned, this scheme entirely different from all other schemes being used in wireless LAN. It is more close to cellular network where all transmissions have to pass through a base station like access point used in polling. Stations cannot communicate directly with each other. They have also to wait for their polling in AP. It causes delay in the network. There is also extra overhead if one station has nothing to send but the AP will poll it in each turn. This scheme is not suitable for ad hoc networks as it based on AP which is against to infrastructure-less network.

3.1.2 Comparison of MAC Algorithms

To conclude the discussion of above described MAC schemes, a brief comparison is to be narrated. Table 3.1 is also highlighting the text. Starting with **CSMA/CA** as it is basic carrier sensing scheme using random back-off algorithm. The standard **IEEE 802.11** is also using this scheme but with addition of DIFS, SIFS and back-off timer. Both of them have failed to solve the hidden and exposed terminal problems.

The **MACA** is based on control packets RTS/CTS. There is no ACK in the method. In MACA, a node overhears an RTS packet it only defers its transmission until corresponding CTS packet is to be received instead of deferring until the end of data transmission. A node overhearing a CTS packet defers its transmission till the end of corresponding data transmission. This is the big difference with **IEEE 802.11 MAC** with RTS/CTS extension. In this standard, any station overhears an RTS or CTS packet, will set an NAV to defer itself from medium access till the end of data transmission and corresponding ACK frame to be received. **MACAW** is modified by adding ACK, Data-

Sending (DS) and Request-for-Request-to-Send (RRTS) frames in MACA. The hidden and exposed terminal problem has been solved to some extent by these three schemes. The chances of collision are still remain, and exposed terminal problem appearing more while using virtual sensing methods.

Polling is the quite different mechanism as compared to all others. It is centralized scheme because an access point (AP) controls all communication between nodes. The nodes cannot transmit at their own will rather AP permits each node turn by turn to send their data packets. It does not use any back-off algorithm. Hence there are no such problems of hidden and exposed terminal.

Table 3.1: Comparison of MAC Algorithms in infrastructure-based WLAN

Algorithms	**Carrier Sensing , RTS / CTS, Polling**	**NAV (virtual sensing)**	**DIFS / PIFS / SIFS**	**Back-off Algorithm**	**Back-off Timer**	With **ACK**	**Centralized**
CSMA/CA	Carrier Sensing	No	----	BEB	No	Yes	No
MACA	RTS/CTS	No	----	BEB	No	No	No
MACAW	RTS/CTS	No	----	MILD	No	Yes	No
IEEE 802.11 with CSMA/CA	Carrier Sensing	No	DIFS / SIFS	BEB	Yes	Yes	No
IEEE 802.11 with RTS/CTS	Carrier Sensing & RTS/CTS	Yes	DIFS / SIFS	BEB	Yes	Yes	No
IEEE 802.11 with Polling	Polling	Yes	PIFS / SIFS	-----	-----	Yes	Yes

3.2 Infrastructure-less WLAN: "AD-HOC Network"

A mobile ad hoc network (MANET) is a wireless network temporarily and dynamically created only by mobile stations (MSs) without using any pre-existing infrastructure. Means there is no base stations or access points like in infrastructure-based WLAN. The Figure 3.9 is showing that all stations communicating with each other without an AP. A MS (laptop, mobile phone, PDA) in this system performs all tasks like access point, router and including its own applications etc. A MS could be in moving state while in ad-hoc network and it can join or disjoin the network any time at its own will. So there is no fix topology. Hence the multiple hops communication exists among the nodes. Each node has a responsibility of relaying packets for others and a packet has to traverse multiple nodes to reach a destination. Such unique features make ad hoc networks distinct from other types of wireless networks.

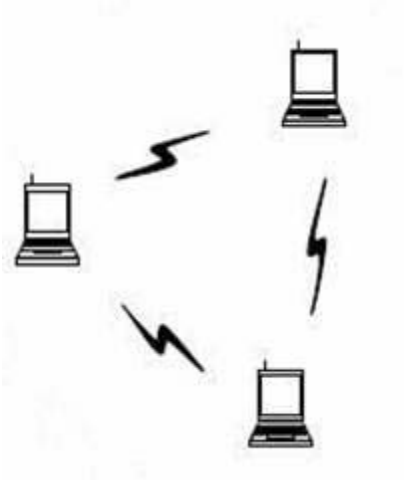


Figure 3.9: Wireless Ad hoc Network

In the following section of the survey, we briefly introduce a variety of MAC protocols that have been used and few are proposed for ad hoc networks. Their techniques have been discussed with some issues.

3.2.1 MAC Algorithms in Ad-Hoc network

MAC Algorithms are classified in two categories here as ad hoc networks either use Omni-directional Antennas (OA) or Directional Antennas (DA).

A. Omni-directional Antenna MAC protocols

i. CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) is one of the earliest multiple access schemes adopted for ad hoc networks after its success in infrastructure-based WLAN. CSMA attempts to avoid collisions by sensing carrier in the vicinity of the transmitter. Collisions however occur at the receivers, not at the transmitter. In an ad-hoc wireless network the performance of CSMA/CA is still limited by the so called hidden and exposed terminals. The scheme has been explained well in section 3.1.1. Thus CSMA does not provide an appropriate mechanism for collision avoidance.

Issues: The well known CSMA/CA is one of the basic medium access algorithms used in wireless networks. Ad-hoc networks also adopted it in very early times. But the major issues of hidden terminal and exposed terminal problems are exist in this area as well. Due to this it does not provide satisfactory results. In addition, CSMA/CA does not support access on priority bases in ad-hoc wireless networks.

ii. MACA / MACAW

To overcome the hidden and exposed terminal problems, the MACA has been introduced for infrastructure-based WLAN. Now it becomes one of the multiple access schemes for ad-hoc networks as well. Its modified version: the MACAW is also being used in this type of network. It basically follows the same RTS/CTS scheme as MACA does. But it introduces some more frames/packtes in the algorithm. Both MACA and MACAW have already been described in section 3.1.1.

Issues: The MACA/MACAW algorithms tried well to eliminate the hidden and exposed terminal problems. But the problem could occur in few cases and causes the collisions; if RTS frames are sent simultaneously by two adjacent nodes or CTS is sent by receiver and at the same time RTS is sent by any hidden node. Moreover, use of control packets creates delay and overhead in the communication. MACAW is using additional packets more than MACA. Particularly the ad-hoc network which is very dynamic and mobile, it needs communication and related response to be very quick and fast. But MACAW is not much suitable for this domain.

iii. IEEE 802.11 MAC

The IEEE standard 802.11 for WLAN is suitable for both infrastructure-based and infrastructure-less WLAN. But IEEE 802.11 offers only asynchronous data service in ad-hoc networks not the time-bounded service. Therefore, in ad hoc network the IEEE 802.11 MAC has been implemented by using CSMA/CA and RTS/CTS techniques. These techniques come under the category of “Distributed Coordination Function” (DCF). The algorithms are well described in the section of infrastructure-based WLAN. As time-bounded service is not supported in ad hoc, so polling scheme could not be applied.

iv. FAMA

In order to solve the problems of MACAW, Garica-Luna-Aceves and Fullmer propose the *Floor Acquisition Multiple Access* (FAMA) protocol. FAMA combines non-persistent carrier sensing with the control packets RTS-CTS, so this is referred as FAMA-NPR (FAMA non-persistent) [6].

In MACAW, the hidden and exposed terminal problem is not completely solved. The RTS-CTS was originally intended to solve that problem but actually there is a chance that these packets can collide themselves. Consider an example that if A sends RTS to B, it is possible that B is also sending RTS to either A or C. Consequently, RTS from A will be collided or lost respectively. On the other hand, if B receives RTS from A and starts replying CTS to it, at same time C can send RTS to B and hence will be a collision at B.

In **FAMA**, the key feature is that the RTS and CTS packets have a larger transmission time than the maximum one-way propagation time between any two nodes in the network [6]. Furthermore, the transmission time of the CTS packet is longer than the transmission time of RTS packet. It enables the CTS packet to dominate the RTS packet. Consequently, if a node A transmits RTS packet and simultaneously neighboring node B transmits CTS, then node A will be able to hear at least part of the CTS and will defer itself. Hence FAMA protocol removes the packet collision in a network with hidden terminals, and it guarantees that a single sender is able to send data packets without collision to a certain receiver at any given time.

Issues: The above narrated MAC algorithm has been successful in order to avoid collision. On the other side of the spectrum, FAMA brings some issues as well. By increasing the transmission times of RTS/CTS the system will become slow in progress. Especially in ad-hoc network which is mobile in nature and its topology changes very quickly, the MAC scheme has to be very fast in order to yield better results. Therefore its throughput is not much high inspite of the fact that it reduces packet collision.

v. DBTMA

Dual Busy Tone Multiple Access (DBTMA) protocol was proposed by Hass and Deng. DBTMA distinguishes itself from other MAC protocols in two aspects: it splits a single channel into two sub-channels, and secondly it uses a pair of transmitting and receiving busy tones to serve the virtual sensing [7].

The busy tone serves two roles. First, it is used as *transmitting busy tone*, which a transmitter sends out through the transmission of its RTS packet. Thus, the RTS will have better opportunity to be successfully received by the intended receiver. Note that the possibility of the collision of two RTS packet still exists, though it has been reduced by transmitting busy tone. In addition to the transmitting busy tone, there is also *receiving busy tone*, which serves the same function as CTS to acknowledge the RTS. Also, it prevents nearby nodes from interfering with current transmission.

Issues: In domain of wireless ad-hoc network the DBTMA improves the system throughput more significantly than previous explained protocols. But the problem of DBTMA is that it requires more complicated hardware than being used in 802.11 to implement the two band busy tones. Also the bandwidth allocated to the two busy tones is negligible, which is not necessarily true under heavy traffic conditions. Finally, it is quite difficult to make this scheme compatible with 802.11 without major modifications in terms of both hardware and software.

Comparison of *OA* MAC Algorithms in Ad hoc

The protocols used with omni-directional antennas are almost same which were used in infrastructure-based WLAN. So, the comparison here would be more or less similar.

Table 3.2: Comparison of ***OA*** MAC Algorithms in Ad-Hoc Networks

Algorithms	Carrier Sensing	RTS/CTS	Increased RTS/CTS Transmission time	Back-off Algorithm	Busy Tone based	Split channel
CSMA/CA	Yes	No	No	BEB	No	No
MACA / MACAW	No	Yes	No	BEB / MILD	No	No
FAMA	Yes	Yes	Yes	BEB	No	No
DBTMA	No	Yes	No	MILD	Yes	Yes
IEEE 802.11 MAC	Yes	Yes	No	BEB	No	No

B. Directional Antenna MAC protocols

Ad-hoc wireless system is becoming more mobile and autonomous day by day. In order to enhance its efficiency, the use of *Directional Antennas* (DA) can be very beneficial. The DA in ad hoc networks can largely reduce the radio interference and so improving the system throughput.

To utilize the directional antennas in better way, the Medium Access Control (MAC) protocols must be redesigned or improved. Because the current MAC protocols, such as the IEEE 802.11 standard, have been designed for omni-directional antennas and therefore cannot work properly with directional antennas [9]. For this purpose some new algorithms have been proposed as explained below.

i. MAC/DA1

This is one of the first efforts to use IEEE 802.11 MAC for directional antennas (DAs). Its key features are:

- There is a usage of *directional RTS* (DRTS) packet.
- *Directional* RTS reduces the chances in which an unintended receiver can overhear the RTS frame and thus significantly relieves the exposed terminal problem [9].
- Also relieving the hidden terminal problem by recording the directions from which the CTS frames are recently overheard and then blocking the antenna elements in the corresponding sectors. The node is allowed to transmit only in the collision free directions. All *CTS* are *omni directional* (OCTS).
- To transmit a directional RTS frame needs to know the direction of the intended receiver, which is referred to as the *location tracking* problem. The MAC/DA1 gives the solution is to equip every node with GPS support and depends on a *beacon* protocol of nodes to exchange location information periodically [9].

This scheme1 improves the performance of system in such a way that two different transmissions can run simultaneously in one network. Considering a scenario in Figure 3.10, node B has to send some data to node C. It starts with directional RTS (DRTS) sending to C. The node C replies with omni-directional (OCTS), that will reach to B and D as well. Then B can send data packet to C and finally will receive an ACK from C. The good aspect here is that node D can complete its communication with node E at same time. After receiving OCTS from C, it will block its directional antenna towards C and can send DRTS to E through DA towards E.

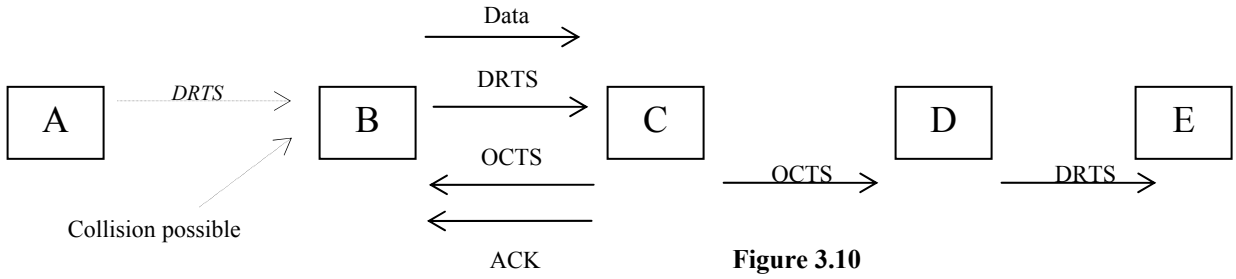


Figure 3.10

However, the drawback of this scheme exists: The node A does not receive DRTS from B as it was directed only towards C. Also it does not receive OCTS from node C either, as A is out range of C. So at that particular time, if A wants to transmit DRTS to B it can do that and hence cause a collision at B. The probability of collision between control packets is quite high in this case. It is even higher than IEEE 802.11 MAC [9].

ii. MAC/DA2

The scheme 2 of DA has the following features:

- It reduces the probability of collision between control packets.
- It uses both types of RTS packets: *directional RTS* (DRTS) and *omni-directional RTS* (ORTS).
- However, the CTS just remain *Omni-directional* (OCTS).
- It uses *on-demand* approach for location tracking.
- It produces the ability of the receiver to determine the direction of arriving frame so that transmitting and the receiving nodes could learn each other's directions.

On-demand approach means the sender decides on run-time whether the DRTS is to be sent to the intended receiver or just ORTS. Assume a node X wants to send something to node Y. If all directional antennas at node X are unblocked then node X will send an ORTS to Y, otherwise X will send just an DRTS provided that DA towards Y is not blocked. If the required antenna is blocked then node X will defer itself until the antenna becomes unblock [9].

For example in Figure 3.11, the node B wants to send data to node C and none of B's antennas are blocked. It will broadcast ORTS packet. Thus packet is received by both nodes A and C. As a result A will block its antenna directing to B. Now considering the case that if node A wants to send a packet to node B, it will defer its transmission until B and C finish there transmission. But if node A wants to send something to node F then it will send DRTS packet towards F provided DA pointing to F is not blocked. Hence it reduces the chances of collision.

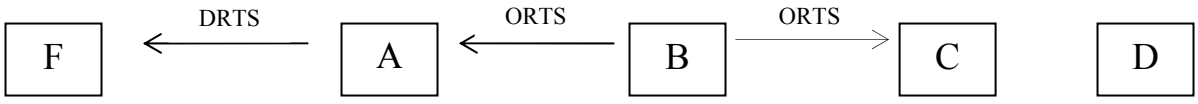


Figure 3.11: Ad hoc Network using Directional and Omni-directional RTS

The scheme 2 is quite successful in reducing the possibility of collision and achieving high throughput. But the drawback is that it also reduces the possibility of simultaneous transmission between two neighboring nodes in a network.

iii. DBTMA/DA

This is the directional antenna version of the DBTMA protocol. Like DBTMA it splits a single channel into two sub-channels and uses the busy-tones, however it uses directional rather than omni-directional busy-tones. By using directional busy tones, it offers the similar feature as in MAC/DA1 of directional RTS packet.

Comparison of *DA* MAC Algorithms in Ad hoc

The above stated schemes have possibly made improvements in wireless ad-hoc networks by getting high system throughput. Although these are proposed schemes and are being evaluated at the moment through various simulation results. Some of the comparisons of *DA* MAC schemes also related to those results.

The MAC/DA1 and MAC/DA2 schemes depend on IEEE 802.11 MAC (using RTS/CTS). Here they use directional RTS (DRTS) with omni-directional CTS (OCTS). Scheme 1 uses only DRTS and OCTS but scheme 2 uses both DRTS and ORTS with OCTS. Scheme 1 allows running two transmissions simultaneously, on other hand scheme 2 reduces the chances of two transmissions at the same time. Possibility of collision between control packets is high in scheme 1 as compared to scheme 2. The system throughput in scheme 2 is significantly higher than scheme 1's throughput. As for as DBTMA/DA is concerned, it is a modified version of DBTMA which was used in ad-hoc using omni-directional antenna. It uses RTS/CTS packets with the addition of directional busy tones. System throughput is high here, but it does not provide facility of running two transmissions simultaneously.

Table 3.3: Comparison of ***DA*** MAC Algorithms in Ad-Hoc Networks

Algorithms	Basic Protocol	Carrier Sensing	Omni directional RTS/CTS	Directional RTS	Directional Busy Tone	On-Demand Location Tracking
MAC / DA1	802.11	Yes	CTS	Yes	No	No
MAC / DA2	802.11	Yes	RTS/CTS	Yes	No	Yes
DBTMA/DA	DBTMA	No	RTS/CTS	No	Yes	Yes

4 Wireless Personal Area Network

The IEEE 802.15 is the standard for Wireless Personal Area Networks (WPANs). It was formed to develop standards for short range wireless devices separated by up to 10 meters, unlike WLAN where devices could be separated by up to 100 meters, and the cellular network that spans over the range of 100 of kilometers. Devices in a PAN may include portable and mobile computers (laptops), cell phones, pagers and other mobile devices. The WPAN is a form of ad hoc network. The notion of IEEE 802.15 was originally created by the *Bluetooth* technology in 1999.

BLUETOOTH is a short-range and low-power wireless technology for small distance up to 10 m. In 1994 Swedish company *Ericsson* initiated some studies to eliminate cables between mobile phones and their accessories. In July 1999, Version 1.0 of Bluetooth specifications came out. Just after that Version 1.0 B published in December 1999 with some corrections and clarifications. The name of Bluetooth belongs to *Harald Blåtand* a Danish king. *Blåtand* in Danish translates as 'Bluetooth' referred to a person having dark complexion. Danish Viking king united Denmark and Norway, and brought Christianity to Scandinavia as well. The name was adopted because Bluetooth wireless technology united some multinational companies and is also unifying entirely two different systems i.e. telecommunications and computing.

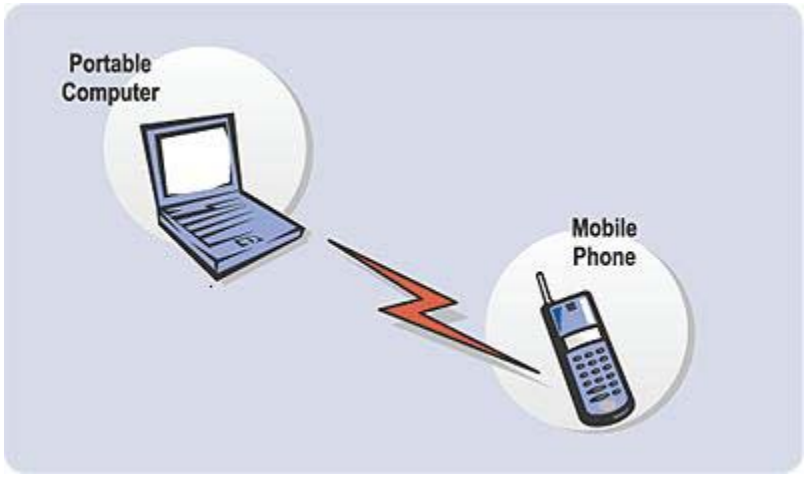


Figure 4.1: Bluetooth Communication

MAC in BLUETOOTH

Bluetooth's MAC scheme is *Frequency Hopping CDMA* (FH-CDMA).

The **CDMA** (code division multiple access) is a well known MAC algorithm of cellular networks. In CDMA, multiple users operate the same frequency and time for communication. But the separation is achieved by assigning each channel its own unique 'code' i.e. orthogonal codes. For this purpose **spread spectrum** techniques are used to spread the whole bandwidth into many channels of smaller bandwidths each, plus guard spaces between the channels. CDMA uses two techniques for spreading the spectrum; *direct sequence CDMA* (DS-CDMA) and *frequency hopping CDMA* (FH-CDMA).

In **FH-CDMA** (frequency hopping CDMA), the total bandwidth B is divided into M orthogonal frequency sub-bands such that bandwidth $B=M$. At each time, the transmitter chooses one of the M bands with equal probability, based on a pseudo-random code sequence that is also known to the receiver. The change of frequency band after certain time interval is called frequency hopping. The receiver has to synchronize with hopping sequence in order to communicate properly. Detail description of CDMA and spread spectrum will come in the section 6 of cellular networks.

The Bluetooth operates in the 2.4 GHz ISM band. The FH divides the total bandwidth into 79 channels (2.402 to 2.480 GHz). Thus bandwidth per channel is 1 MHz. Each device performs frequency hopping with 1600 hops per second. A Bluetooth device (master) that wants to establish the connection determines the unique hopping pattern. This sequence is based on pseudo-random code and is known to all other Bluetooth devices (slaves). The clock of the master defines the phase in the hopping sequence. Any other Bluetooth device (slave) wants to communicate with the master must be synchronized to that unique hopping pattern determined by the master device ID; a 48-bit worldwide unique identifier [1]. Furthermore, the slave has to adjust also its internal clock according to master clock in order to participate in the piconet.

The *piconet* is the collection of Bluetooth devices which are connected to each other. There must be at least two devices to form a piconet and maximum eight devices can take part in it. Only one device acts as a master (M) that initiates the connection process. All other devices connected to that device are called slaves (S).

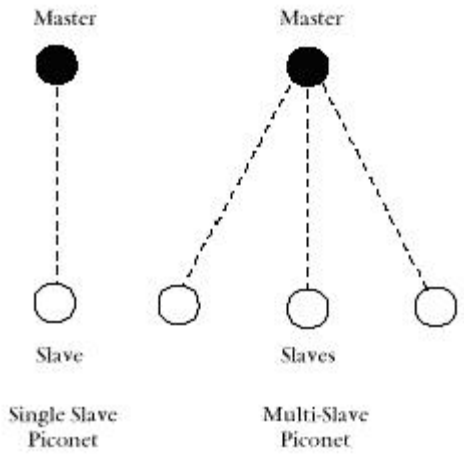


Figure 4.2: Bluetooth Piconet

The Bluetooth specification supports both point-to-point and point-to-multipoint connections, hence two or more piconets can be linked together to form a *scatternet*. A device in one piconet can become a part of another piconet as well. Interestingly, a slave in one piconet may function as a master in another piconet, but it is impossible for a master of one piconet to act as the master of another piconet at same time, it has to become a slave for that one [1]. Addition to that, communication is possible only between the master and one or more slaves.

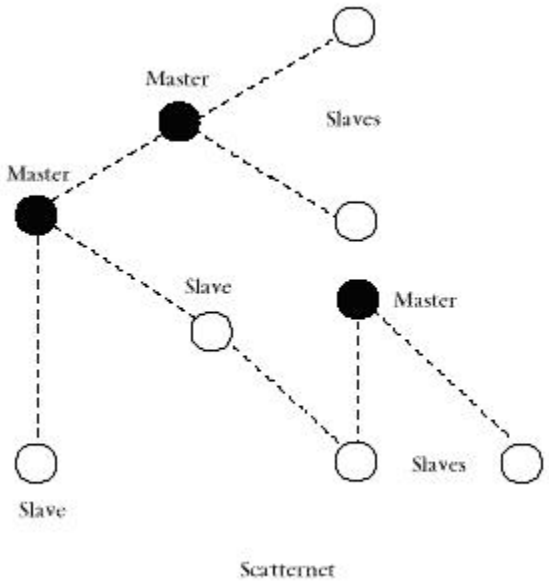


Figure 4.2: Bluetooth Scatternet

Bluetooth has now become the IEEE based standard **802.15.1**

Advantages:

Bluetooth is an invention and new notion in the field of wireless. It has integrated the two technologies. Bringing the world more close and advance. It provides comfortable use of computer and mobile accessories by removing the cables. Also it is a new thing in the software which opens bright opportunity for software programmers.

Disadvantages/ Issues:

Originally Bluetooth specifications were not according to IEEE standards. It was new but also a complicated technology in the market. Initially it was hard to understand and to adopt it in the running systems. Therefore the devices were expensive as well. Bluetooth being subset of WLAN and a part of ad hoc networks its MAC scheme is quite different in nature as compared to original WLAN MAC protocols. As in WLAN mostly the MAC schemes based on carrier sensing and virtual sensing but Bluetooth MAC is CDMA based which is rather a cellular network technique. Hence it was closer to telephony networks and not supportive to computing environment much. But now companies are producing its more computer related accessories.

5 Wireless Sensor Network

A wireless sensor network (WSN) consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and certain level of intelligence for signal processing and communication of the data. WSNs are becoming more functioning as they are used in military to detect and gain information about enemy movements, explosions etc., wireless traffic sensor networks to monitor vehicle traffic on highways, security system using sensors for target detection and tracking and also used in tactile system, ubiquitous computing etc. Specifically in WSNs, nodes coordinate locally to perform data processing and deliver messages to a common sink or cluster.

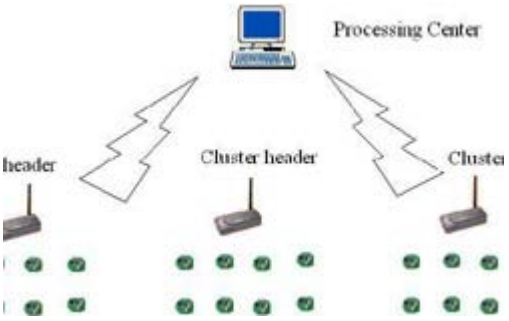


Figure 5.1: A Sensor Network

5.1 Reasons for Well-defined MAC in WSN

Sensor nodes are more energy consuming as they have to be remain active all time to detect and process the required information. They have to listen, hear and monitoring the proceedings continuously. Therefore, the task of MAC algorithms for WSNs is to provide such a mechanism that sensor nodes could reduce the energy consumption, idle listening, overhearing etc. and enhance the output of the sensor network as well.

5.2 MAC Algorithms in WSN

Hence, to design a good MAC algorithm for wireless sensor network, the above mentioned reasons must be kept in mind. The most important is the energy efficiency. There must be energy efficient protocols in order to enhance the duration of the network system. A good MAC algorithm should also be finely accommodative to the rapid changes occur in sensor network. These changes are the addition of new nodes, change in network size and the network topology as well. Other typical important things are throughput, latency and bandwidth utilization [10].

The following are the well-defined MAC algorithms for wireless sensor networks. In addition to that, their advantages and disadvantages will also be presented.

i. S-MAC

The basic concept of Sensor-MAC (S-MAC) algorithm is the synchronization management and sleep-listen schedules based on these synchronizations. It uses cluster approach for communication, where some nodes close to each other form a virtual cluster. One of these nodes acting a leader called cluster-head. Actually, the clusters are formed to set up a common sleep-listen schedule. It is possible that two neighboring nodes reside in two different virtual clusters, but they wake up for listening on the schedules of both clusters. This is the main drawback of S-MAC that the node has to follow two different schedules. That results in more energy consumption via extra listening and overhearing. Schedule information is exchanged by broadcasting periodically the SYNC packet to immediate neighbors. The period of sending a SYNC packet is called the synchronization period. Carrier sensing is also used for collision avoidance. Furthermore, RTS/CTS packets are used for unicast type data packets. The long messages are divided into frames and sent in burst. In this technique, the node which overhears its neighbor's transmission wakes up for a short time at the end of the transmission. Hence, if the node is the next-hope node, its neighbor could pass data immediately [11].

Advantages: The sleep schedules reduce energy to some extent. It avoids collision by using carrier sensing. Its implementation is simple. Moreover, synchronization packets update the listen-sleep schedules, which help in better throughput. And the latency is minimized among the nodes close to each other.

Disadvantages: Since the neighboring nodes have their own sleep-listen schedules, which increase the latency and throughput. The sleep-listen schedules are predefined, which decreases the efficiency of the algorithm under variable traffic load. Broadcast data packets do not use RTS/CTS which increases the probability of collision.

ii. SIFT

SIFT is a MAC algorithm for event-driven wireless sensor networks (WSNs). The basic behind SIFT is that when an event is sensed by N nodes, then the first R of N messages is the most important and has to be transmitted with low latency. SIFT is a contention-window based MAC protocol. Each node picks a random contention slot (a value) for transmission. If no node starts transmission in the first slot of the window as there is same value for all, then each node increases that value exponentially for the next slot assuming that the number of competing nodes is small. SIFT is also randomized CSMA protocol. Since it is based on contention slot protocol, it is proposed to co-exist with other MAC protocols like S-MAC [12].

Advantages: All nodes have same priority in the network. All are active at the same time. No sleeping schedule. Hence it increases the efficiency and achieves very low latency.

Disadvantages: As nodes remain busy in sensing the event and never sleep, so they consume high energy. There is idle listening and overhearing as well. Moreover, it is a complex system to implement.

iii. DMAC

DMAC is the Data-gathering MAC algorithm for wireless sensor network (WSN). The goal of DMAC is to be an energy efficient and low latency MAC scheme. The most significant feature in DMAC is data-gathering from sensor nodes to the sink. It is held in tree structure *data-gathering tree*. Data flow in data-gathering tree is unidirectional from sensor nodes to sink. The sink is the ultimate destination. Only sensor nodes forward the received packet to the next hop. Hence, during receive period of a node, its entire child nodes have transmit periods [13].

Advantages: DMAC achieves quite reasonable latency by assigning subsequent slots to the nodes that are successive in the data transmission path. DMAC is considered famous one to have low latency as compared to other MAC protocol proposed for WSN.

Disadvantages: There are no measures to avoid the collisions. It can be occurred, as neither carrier sensing nor RTS/CTS packet have been used. Moreover, the data paths are not known in advance, which resists the construction of data-gathering tree.

iv. T-MAC

Basically, the algorithm has been proposed to overcome the deficiencies of S-MAC algorithm. The Timeout-MAC (T-MAC) improves the results of S-MAC under variable traffic load. In T-MAC, the listening time ends when no event occurs for a certain amount of time: a threshold time defined in the algorithm. It accepts the variable load and heavy traffic as well. Overall it gives the better results [14].

v. DS- MAC

It is also a step of improvement for S-MAC algorithm. Dynamic Sensor-MAC (DS-MAC) brings the idea of dynamic duty cycle to be added in the S-MAC algorithm. All nodes start with the same duty cycle. Within the synchronization period, all nodes share their one-hop latency values (time between the transmission and its reception of a packet into the queue). When a receiving node notices that average one-hop latency value is high, it decides to decrease its sleeping time and announces it within synchronization period. Consequently, when a sender node receives the signal of decrement in sleeping period, it checks its queue for packets destined to that receiver node. If there is one, it decides to double its duty cycle [15].

5.3 Comparison of MAC in WSN

The elaborated algorithms for WSN are more technical than for other type of networks. It is obvious that WSN are the emerging, challenging and most demanding nature of network. On the other hand, its MACs are critical type of protocols. The discussed algorithms are enough so far to understand their behavior in WSN. Mostly all these MACs are using carrier sensing but not virtual sensing as fast response is required. Some of them are energy efficient. The sleep-listen schedule is the key feature in WSN's MACs; through this they save a lot of energy. There is also an *Accommodative* property shown in the Table 5.1 which means the ability to adopt the changes dynamically occurred in the network.

Table 5.1: Comparison of MAC Algorithms in Wireless Sensor Networks

Algorithms	Basic Concept	Carrier Sensing	Synchronization based	Sleep / listen schedule	Cluster approach	Energy efficient	Accommodative
S-MAC	Synchronization management	Yes	Yes	Yes	Yes	No	Good
SIFT	Event driven	Yes	No	No	No	No	Good
DMAC	Data gathering	No	No	Yes	Yes	Yes	Weak
T-MAC	Listening Time Threshold	Yes	Yes	No fixed schedule	Yes	Yes	Good
DS-MAC	Dynamic duty cycle	Yes	Yes	Yes	Yes	Yes	Good

6 Wireless Cellular Network

There has been a tremendous growth in wireless cellular technology over the last decade. The term *cellular* refers that the certain geographical area is divided into small areas called **cells**. Each cell contains a **base station** (BS). The BS transmits and receives the signals to and from the **mobile stations** (MS) in its cell. The coverage area of a cell depends on transmitting power of BS, the transmitting power of MS, buildings and mountains in a cell etc. Each base station is connected to **mobile switching center** (MSC) as shown in the Figure 6.1. The MSC is then connected to Public Switched Telephone Network (PSTN) which serves the functionalities as done by conventional telephone switching center [4].

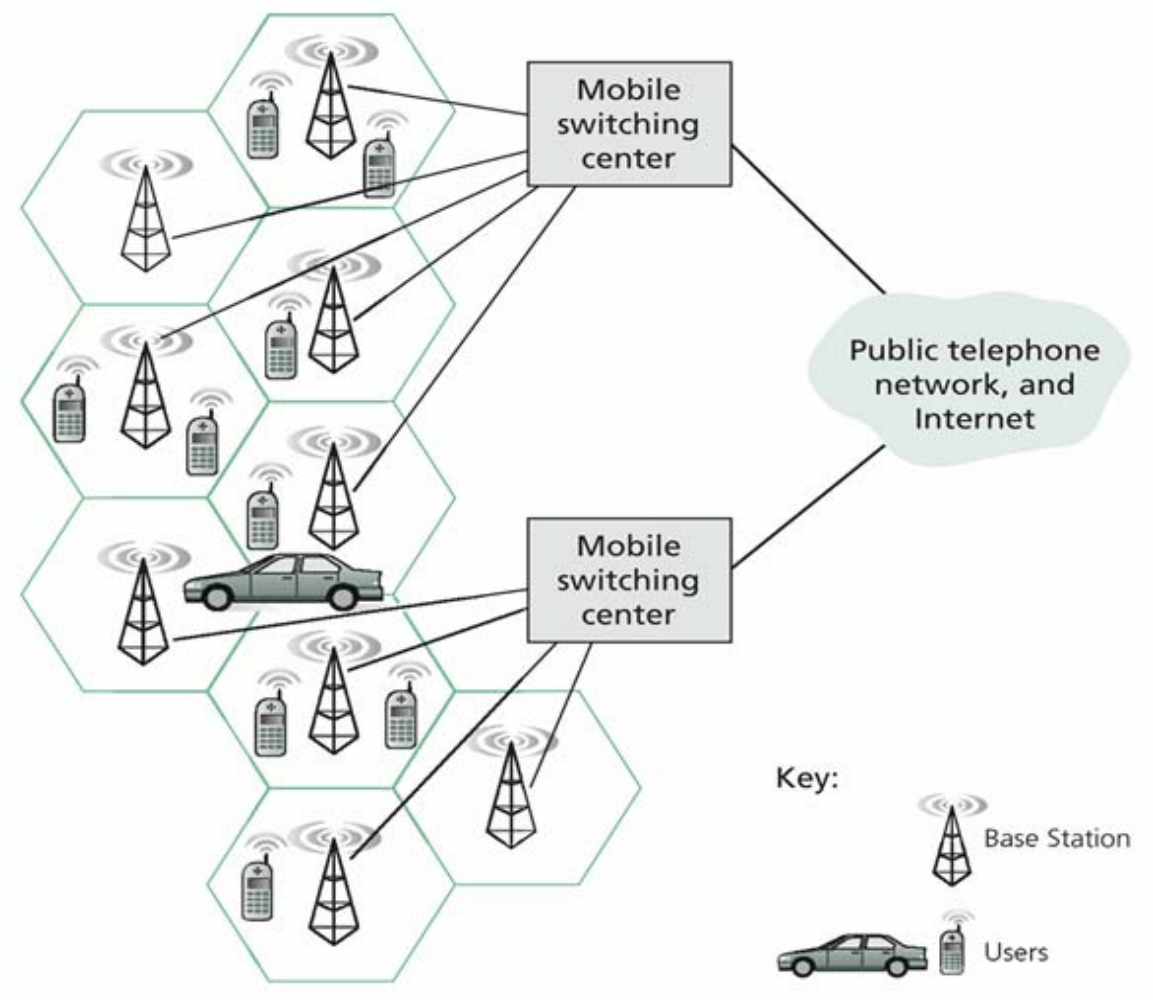


Figure 6.1: Cellular Network Architecture [4]

As cellular network is a type of telecommunication network, so it requires the communication like in ordinary telephone system; talking and listening simultaneously. This mechanism is called *Duplexing*. In cellular network the Duplexing can be done by using either frequency or time division duplexing.

Frequency Division Duplexing (FDD): *FDD* provides two different frequencies bands to each user; one is for uplink channel and other for downlink. The uplink channel is responsible for data flow from mobile station to base station, and downlink channel is from base to mobile station. In FDD, actually a duplex channel is consists of two simplex channels (forward and reverse) at the same time.

Time Division Duplexing (TDD): *TDD* uses time in order to provide uplink and downlink. In TDD, multiple users utilize a single radio channel by taking turns in different time-slots. Each duplex channel has both uplink time-slot and a downlink time-slot for bidirectional communication. Thus, TDD provides two simplex time-slots on same frequency.

6.1 MAC Protocols in Cellular Networks

The cellular network has different requirements for sharing a common medium. Its network and users are spread over the cities, a country or even more than one country. The users must be allowed to use their mobile phones calls at their own will. It should not be case that they remain busy in sensing the carries or exchanging the control packets like in WLANs. Thus, the sharing of medium access in cellular network can be achieved by allocating each user a different frequency or time-slot in order to access the channel at any time as same as in conventional telephone system. Particularly in cellular networks, sharing a common medium by several users is dependent to four basic dimensions: space, time, frequency and code.

i. FDMA

The *frequency division multiple access* (FDMA) divides the whole frequency available into several frequency bands or channels depends on the number of users. These bands are non-overlapping and unique in nature. A user is assigned a unique frequency band as soon as new mobile phone connection is established. Sender can use a certain frequency continuously at any time. Each channel in FDMA is a pair of frequencies by using FDD; one frequency is for uplink, while other is used for downlink. Since it uses duplexing, so both caller and receiver can communicate at the same time. [2]. Overall it is a less complex system. The Figure 6.2 is describing the protocol clearly if there are six users than whole frequency available is sub-divided into six sub-channels each having different frequency. They are unlikely to interference each other.

Issues: On the other side of spectrum, this scheme has also some issues. Allocating a separate frequency to each user makes the algorithm inflexible and confined the number of users. It is also the sever wastage of frequency resource as it is dedicated to the users for unlimited time period, but the users utilize it for a few minutes per day or so.

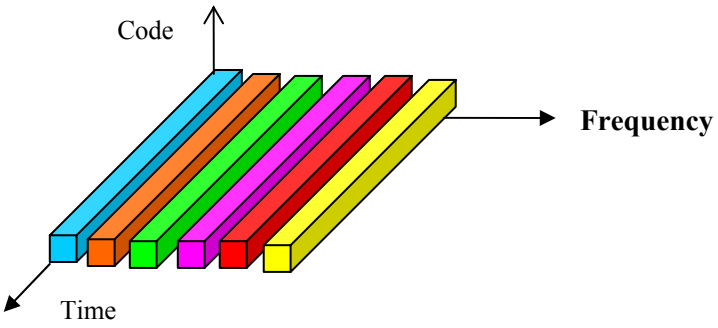


Figure 6.2: Frequency Division

ii. TDMA

It is much more flexible scheme as compared to FDMA. In *time division multiple access* (TDMA) the channel is divided into time-slots. Each time slot allows one user to either transmit or receive data. The frequency remains same for all users but separation is achieved through division of time i.e. time-slots, as in the Figure 6.3 the frequency is same for all 6 channels but total time is divided into 6 slots.

Two or more time periods can interfere each other, and to avoid this precise synchronization is necessary. This is done by base station which reserves the time slot at right moment for different callers. In TDMA system the data is transmitted in a ***buffer-and-burst*** method [2]. During one time-slot only the part of whole data is buffered and burst to destination and remaining data is buffered in the next time-slots accordingly. Thus, the transmission is not continuous for all users. But time difference between two time-slots is so small (in micro-seconds) that it is not felt by a user e.g., GSM system based on TDMA and a caller using GSM, does not feel any delay due to time-slots. The data of different users is buffered into repeating frames. The frame consists of number of slots. The receivers are also required to be synchronized for each data burst. TDMA/TDD separates the time-slots for uplink and downlink procedure by using different frames. But if TDMA/FDD is the system, then similar frame would be used for uplink/downlink transmission, but carrier frequency would be different for both links [2].

Issues: Besides a successful scheme it has main drawback of time synchronization where users require precise clocks. The receiver does not need to tune for the frequency rather just to listen at right point of time. Data could be lost as it is sent in different frames.

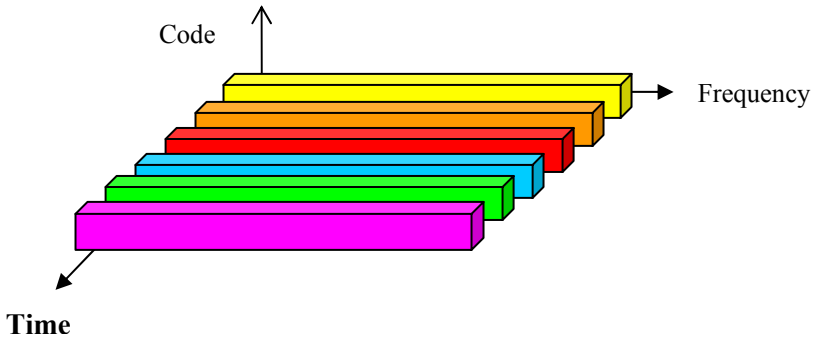


Figure 6.3: Time Division

iii. FDMA / TDMA

One more multiple access scheme is possible by combining Frequency and Time division multiplexing together. The subdivision is required in both time and frequency dimensions. Now a channel can use a certain frequency band for a certain amount of time. As time-slot moves to next, the frequency changes too during a transmission. This change of frequency is called *frequency hopping*. The most famous cellular system GSM uses this MAC technique for transmission between mobile station and base station.

Issues: A main disadvantage is the quite small frequency is available only for a short amount of time. The more complicated side is the receiver, it has to know the sequence of frequencies used by sender and also the appropriate time-slots are to be selected as well.

iv. SDMA

The task of *space division multiple access* (SDMA) is to allocate a separate space to each user for wireless communication with a minimum of interference and a maximum of channel utilization. SDMA assigns space, time, frequency and code to each communication channel. Actually, it is never used alone but always works together with any other technique like time, frequency or code division etc. The space division implies the interference range of each channel [1]. For example, the range of FM radio station is limited to certain region. The FM 100 channel is running in both Sweden and Pakistan with same frequency but different spaces which are limited to their respective countries.

In cellular networks using SDMA, each mobile phone is assigned an appropriate base station. The Mobile phone may receive signals from several base stations. But the (SDMA) MAC algorithm chooses the required one among all signals considering the time, frequency or code. The down link procedure is strong as base station has entire control over the power of all transmitted signals. In case of uplink, the transmitted power is dynamically controlled to avoid interference with other signals. The transmitted power is limited in mobile phones due to the use of small batteries.

Issues: One of main problems lies in SDMA is that it has limited transmission range. Also, it is the combination of two or more techniques. Allocating just space to channels does not work correctly, rather it uses different frequencies, time slotting etc. besides different spaces. In SDMA, another issue comes up if two or more channels start running within same space having same time-slots, codes or frequencies then the channels will definitely fail to run successfully.

v. DSMA

The *digital sense multiple access* (DSMA) algorithm is used for packet data transmission service: *Cellular Digital packet Data* (CDPD). It is a type of slotted p-persistent CSMA mechanism. There is only one Uplink/Downlink pair available per slot for data transmission in each CDPD cell. The downlink channel is easy to manage because base station is the only sender per cell. On the contrary, the uplink channel is critical as there are number of mobile stations (MSs) trying to send data at same time. When MS wants to

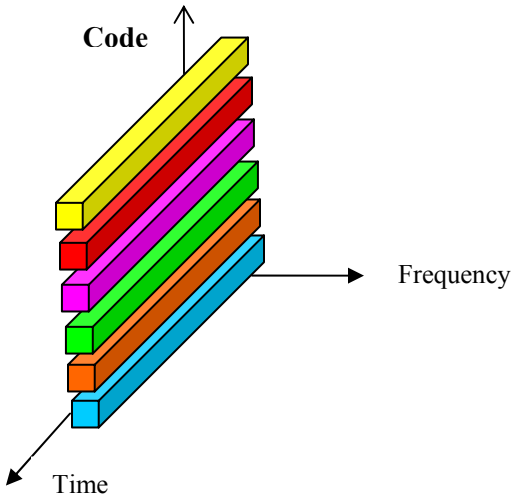
send packet it senses the downlink for a flag bit indicating whether the uplink is busy or idle at the moment. If it is free then data is sent and acknowledgment from base station is received. But if uplink is busy then MS does not wait for next slot rather it skips the random number of slots and tries again [3].

Issues: DSMA is one of the pioneer medium access schemes for cellular network. It used to serve well when number of users was small. Because this scheme is based on carrier sensing and uses few slots, using carrier sensing while making a phone call is not the proper way of accessing the medium. But now cellular networks have grown tremendously in all over the world and it is rendering huge amount of people. Thus DSMA is no more a suitable choice.

vi. CDMA

Code division multiple access (CDMA) is relatively the new and advance medium access algorithm for wireless networks. Initially it has been used in military applications, now this system is a part of commercial cellular networks as well. In CDMA transmission all channels use same frequency at the same time, but separation is achieved by assigning each channel a unique '**code**' e.g., orthogonal codes. These unique codes provide better security against interference and tapping [1]. The critical tasks like how to find suitable codes, performing encoding and decoding are all done by ***spread spectrum*** technique shall be explained after issues.

Issues: The main issue is the high complexity at receiver side. Assigning different codes to each sender usually does not cause problems, but receiver faces some complications. Firstly, the receiver has to separate the original signal from background noise composed of other signals and environment. Secondly, receiver must know the code used by sender, and also must be precisely synchronized with sender in order to perform decoding correctly. *Power control* is another issue in CDMA. An optimum power control is required while the signal reaching the destination so that receiver could detect the original signal as well as the desired codeword. Otherwise decoding cannot be applied properly. Power control is implemented at base station.



Spread Spectrum:

The narrowband signal of CDMA is multiplied by a very large bandwidth signal; resulting signal is called the *spread spectrum*. The spread spectrum is a pseudo-noise or pseudorandom code sequence. Each user has its own pseudorandom code which is orthogonal to all other codes. These codes are basically random binary sequence. There are two ways of spreading the spectrum;

a) *Direct Sequence Spread Spectrum*

The Direct Sequence Spread Spectrum (DSSS) system uses chipping sequence for spreading the spectrum. The chipping sequence is a binary code which is usually called pseudo-noise sequence; generated as a unique code each time when user has to send the signal. While using DSSS, the user data (bit stream) is taken and then performed an XOR with the chipping sequence. Each bit of user is XOR with whole sequence code periodically. For example the user data is 01, and the chipping sequence is 0110101. The result of XOR (resulting signal/spread spectrum) would be: 0110101 1001010. The resulting signal is then modulated and finally transmitted to the receiver. The receiver side is more complex than sender particularly in spread spectrum systems. The receiver has to perform demodulation first in order to get original spread spectrum signal. Next is the critical part to know the original chipping sequence to perform XOR with receiving spread spectrum signal. Actually the transmitter and the receiver are synchronized with the same chipping code. The receiver calculates the code from receiving signal. After having the required code, the XOR is performed and got the original message. The spreading signal was 0110101 1001010, code is 0110101 and the result of XOR = 0000000 1111111. Each seven resulting bits representing the one original bit, hence the data is 01. In this way, the DSSS works nicely depending on the codes [1].

b) *Frequency Hopping Spread Spectrum*

The Frequency Hopping Spread Spectrum (FHSS) system splits the total available bandwidth into several sub-channels with smaller bandwidth each. While communication the transmitter and the receiver stay on one of these sub-channels with a certain frequency for small amount of time and then hop to another sub-channel. This implies that, the signal hops from sub-channel to sub-channel and transmitting short bursts of data on each channel for a certain period of time. The pattern of changing the channels is called the **hopping sequence**, and time spent on each channel is called **dwell time**. The system has implemented both FDM and TDM. The sender and the receiver must be synchronized to the hopping sequence. FHSS can work in either of two ways; slow hopping and fast hopping. In *slow hopping* the transmitter uses one frequency (one sub-channel) for several bits, e.g., the transmitter sends first three bits of data by using frequency f 2. For *fast hopping* the transmitter changes the frequency several times to transmit a single bit, e.g., the transmitter uses three frequencies f1, f2, f3 (hops three sub-channels) during one bit. Fast hopping has been implemented in Bluetooth, whereas slow hopping in GSM [1].

vii. WCDMA

WCDMA stands for *Wide-band CDMA*. It has been adopted as a medium-access technology for the *universal mobile telecommunications system* (UMTS). UMTS is the well known third-generation (3G) cellular network. WCDMA is basically a CDMA protocol but with large bandwidth and high bit-rate data services. The data rate has been enhanced to 2 Mbps as it was 14.5 Kbps in CDMA. Thus it is providing improved services to users. These services include high quality data, streaming music, video streaming, multimedia and also wireless access to the Internet. It renders high spectrum efficiency and high quality of services as well. An important feature of WCDMA is the dynamically channel switching; as WCDMA signal can switch to a GSM downlink signal on run time and vice versa. Furthermore, it is compatible to GPRS, IS-136, EDGE [2].

Table 6.1: Key differences between WCDMA and CDMA

	WCDMA	**CDMA (IS-95)**
Carrier size	5 MHz	1.25 MHz
Data rate	2 Mbps	14.5 Kbps
Chip rate	3.84 Mcps	1.2288 Mcps
Inter-system Handoff	Handoff to GSM	Handoff to AMPS
Technology	Digital Packet Switched	Digital Circuit Switched
Power control	1500 Hz	800 Hz
Generations of wireless telecommunication	3 G	2 G

6.2 Comparison of MAC protocols

The different techniques and mechanisms have been deployed in domain of cellular network. The protocols used here are more versatile in nature. There is no one basic mechanism that belongs to all protocols, rather all have distinct features. TDMA makes time-slots for better sharing of medium, FDMA splits the total bandwidth into sub-channels of different frequency each, CDMA produces unique codes for each user with help of spread spectrum technique, SDMA is applied in separate spaces and DSMA senses the carrier before transmitting the uplink data etc. Furthermore, the protocols are

combined together to form a another MAC protocol like TDMA/FDMA work together in most famous GSM network, and both SDMA and DSMA are the combination of two or more schemes as well. The CDMA has an edge that it can add number of users without any upper limit, because it uses single channel (same frequency and time) but with different codes which has abundant capacity. On the other hand, TDMA and FDMA divide total available time and frequency respectively. The number of users is confined to either total number of time-slots or number of sub-channels with different frequencies each. If all time-slots or sub-channels are allocated to users then a new user cannot be added in the network. The table below is representing some more comparisons of protocols.

Table 6.2: Comparison of MAC protocols in Wireless Cellular Networks

Algorithms	**Basic concept**	**Multiple sub-channels**	**Single channel**	**Combination with more schemes**	**Limited no. of users**	**Network system**
TDMA	Total time of channel divided into time-slots	Yes , multiple sub-channels as many as time-slots	No	No	Yes, limited to no. of time-slots	GSM
FDMA	Total frequency of channel divided into sub-bands	Yes, multiple sub-channels as many as sub-frequency bands	No	No	Yes, limited to no. of sub-frequency bands	AMPS
SDMA	Separate space is allocated to each user	No	Yes	Yes, with TDMA/FDMA or CDMA	No	----
DSMA	Type of slotted p-persistent CSMA	Yes , multiple channels as many as time-slots	No	Yes, with TDMA / CSMA	Yes	CDPD
CDMA	Orthogonal codes using spread spectrum	No	Yes	No	No limit	IS-95
WCDMA	CDMA technique with larger bandwidth	No	Yes	No	No limit	UMTS (3 G)

7 Comparing Wireless Networks Types with respect to MAC Techniques

Eventually, the survey on different medium access control algorithms and protocols has been explicated. They were presented according to their respective type of the wireless networks. To conclude the report, a comparison of various types of wireless networks with respect to MAC algorithms is to be discussed. Here the algorithms or protocols will be considered on their average behavior in the particular network.

The MAC schemes in infrastructure-based WLAN are slightly dissimilar to schemes used in ad-hoc wireless network. Although in both networks, the schemes based on carrier sensing, virtual sensing and use back-off algorithms, but the major difference is the polling mechanism which is used in infrastructure-based WLAN but not in ad-hoc network. It is so because the polling scheme is dependent to the infrastructure-based network. Furthermore, the ad-hoc network is using the directional antenna (DA) medium access schemes unlike to all other wireless network types. The WPAN, a form of ad hoc network, is using frequency spread spectrum with CDMA as a MAC scheme. The MAC algorithms used in WSN are more versatile but most of them have common features like carrier sensing, sleep-listen schedules, cluster approach and should be energy efficient. Whereas the MAC schemes of cellular network are partitioning protocols. They do not use carrier sensing, virtual sensing or cluster approach etc., rather they divide the channel into several sub-channels by time, frequency, space or code division etc. for users. The table is also the highlight of the comparison.

Table 7.1: Comparison of Networks w.r.t MAC Techniques

WIRELESS NETWORKS	**Carrier Sensing** or **Virtual sensing (NAV, RTS/CTS)**	**Back-off Algorithms**	**Directional Antennas**	**Sleep - Listen schedules**	**Polling / Cluster approach / BS based**	**Time, Frequency, Space** or **Code Divisions**
WLAN infrastructure-based	using both type of sensing	Yes	No	No	Polling based on AP	Time division
Ad-hoc network	using both type of sensing	Yes	Yes	No	------	Time division
WPAN	No	No	No	No	-----	frequency, time and code divisions
WSN	Carrier sensing	No	No	Yes	Cluster approach	-----
Cellular Network	No	No	No	No	Base station based	All used

8 CONCLUSION

We have gone through a detailed explanation with many comparisons of MAC protocols. Each network type has its own demand for its medium access control technique. It has been superb learning and exposure of different types of wireless networks as well as their requirements particularly for MAC schemes. So, it was nice opportunity to learn in-depth about various MAC schemes or mechanisms. In addition to all, the upcoming feature is **integration** of technologies. Since the Bluetooth has successfully integrated the computing and telecommunication industry. Bluetooth itself is a form of ad hoc network and it also works well with infrastructure-based WLAN. The WSN works in both fashions as well. Hence, different types of wireless technologies are going to communicate with each other in near future. The newly proposed MAC schemes are mostly focusing on CDMA and spread spectrum technologies.

Future Work

The currently used IEEE standard 802.11 for **WLAN** is actually the 802.11b version. However, in future the upcoming work is 802.11e standard. This new version is bringing enhanced MAC. This MAC is offering QoS in both DCF and PCF operations. The new protocol is also going to provide access categories for different applications such as audio, video or media steaming etc. The newly proposed MAC algorithms for **Ad hoc** networks are CDMA-based. For **WSN** the proposed MAC algorithms are mostly TDMA-based. In **cellular network** the new version of WCDMA Release - 5 which is completely IP-core, has been published. It would most likely be the cellular network system of 3.5 G.

9 ACKNOWLEDGMENTS

First of all, I would like to thank my thesis supervisor Dr. Jerry Eriksson who really managed and guided me well from his precious time. I am also quite grateful to Dr. Per Lindström who has always been very kind and helpful to all international students in computing science department of Umeå University. Thanks to all professors of the University who taught me during last twelve months or so. I am especially thankful to my parents, relatives and all professors who have been supporting and teaching me throughout my career. Finally, I acknowledge the cooperation from my all colleagues who studied with me at school and university levels.

10 APPENDIX - Acronyms

3 G / 2 G	Third Generation / Second Generation
ACK	Acknowledgment
AMPS	Advance Mobile Phone System
AP	Access Point
B	Back-off (counted)
Br	Back-off remaining
BS	Base station
BEB	Binary Exponential Back-off
CSMA	Carrier sense with multiple access
CA / CD	Collision Avoidance / Collision Detection
CDMA	Code Division Multiple Access
CF	Contention Free
CTS	Clear to Send
CW	Contention Window
DA	Directional Antenna
DFWMAC	Distributed Foundation Wireless MAC
DS	Data Sending
DIFS	DCF inter-frame spacing
EDGE	Enhanced Data rates for GSM Evolution
FAMA	Floor Acquisition Multiple Access
FDD	Frequency Division Duplex
FM	Frequency Modulation
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISM	Industrial Scientific Medical
MAC	Medium Access Control
MACA	Multiple Access with Collision Avoidance
MACAW	Multiple Access with Collision Avoidance for Wireless
MILD	Multiplicative Increase and Linear Decrease
MS	Mobile Station
NAV	Network Allocation Vector
OA	Omni-direction Antenna
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PIFS	PCF inter-frame spacing
SIFS	Short inter-frame spacing
TDD	Time Division Duplex

11 REFERENCES

[1] Schiller, J., "*Mobile Communication*", 2nd Edition, Addison Wesley (2003)

[2] Rappaport, T.S., "*Wireless Communication principle and practice*", 2nd Edition, Prentice Hall (1996)

[3] Tanenbaum, A.S., "*Computer Networks*", 3rd Edition, Prentice Hall (1996)

[4] Kurose, J.F., Ross, K.W., "*Computer Networking - A Top Down Approach*", 3rd Edition, Addison Wesley (2004)

[5] Vaduvur B, Alan, Scott S, Lixia, "*MACAW: a media access protocol for wireless LAN's*", Proceedings of the ACM SIGCOMM, London, Pages: 212 – 225, 1994

[6] C. L. Fullmer, J.J. Garcia-Luna-Aceves, "*Floor Acquisition Multiple Access (FAMA) for Packet-Radio Networks*", Proceedings of the ACM SIGCOMM Cambridge, MA, Pages: 262 – 273, 1995

[7] Zygmunt J. Haas, Jing Deng, "*Dual busy tone multiple access (DBTMA) - a multiple access control scheme for ad hoc networks"*, IEEE Transactions on Communications, Vol. 50, Pages: 975 – 985, June 2002

[8] Zhuochuan H, Chien-Chung S, Chavalit S, and Chaiporn J, "*A busy-tone based directional MAC protocol for ad hoc networks*", IEEE MILCOM, Vol. 2, Pages: 1233 – 1238, 2002

[9] Y.-B. Ko and N. H. Vaidya, "*Medium access control protocols using directional antennas in ad hoc networks*", in IEEE INFOCOM, Vol. 1, Pages: 13 – 21, 2000

[10] http://www.eyes.eu.org/sensnet.htm

[11] W. Ye, J. Heidemann, D. Estrin, "*Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks*", *IEEE/ACM Transactions on Networking*, Volume: 12, Issue: 3, Pages: 493 - 506, June 2004

[12] K. Jamieson, H. Balakrishnan, and Y. C. Tay, "*Sift: A MAC Protocol for Event-Driven Wireless Sensor Networks"*, MIT Laboratory for Computer Science, Tech. Rep. 894, May 2003

[13] G. Lu, B. Krishnamachari, C.S. Raghavendra, "*An adaptive energyefficient and low-latency MAC for data gathering in wireless sensor networks*", Proceedings of 18th International Parallel and Distributed Processing Symposium, Pages: 224, 26-30 April 2004

[14] T.V. Dam and K. Langendoen, "*An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks"*, The First ACM Conference on Embedded Networked Sensor Systems (Sensys'03), Los Angeles, CA, USA, November 2003

[15] P. Lin, C. Qiao, and X. Wang, "*Medium access control with a dynamic duty cycle for sensor networks"*, *IEEE Wireless Communications and Networking Conference*, Volume: 3, Pages: 1534 - 1539, 21-25 March 2004