IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 05, Issue 02 (February. 2015), ||VX|| PP 55-64

A Survey on IEEE Standards for Mobile Ad Hoc Networks

K. Praveen Kumar Rao[1], Dr. K. Kalaiarasi[2]
[1]*Research Scholar, Department of Computer Science & Engineering, Vel Tech Dr. RR & Dr. SR Technical University, Avadi, Chennai, India*
[2]*Dr. K. Kalaiarasi, Associate Professor, Vel Tech Dr. RR & Dr. SR Technical University, Avadi, Chennai, India*

Abstract – Mobile Ad Hoc Networks (MANETs) are complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self – organize into arbitrary and temporary " ad hoc " network topologies, allowing people and devices to internetwork in areas with no pre – existing communication infrastructure. Adhoc networking concept is not a new one, having been around in various forms for over two decades. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The growth of laptops and 802.11 / Wi – Fi wireless networking has made MANETs a popular research topic. The introduction of new technologies such as IEEE 802.11, 802.15, 802.15.4, 802.16, 802.20 are helping to enable eventual commercial MANET deployments outside the military domains. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET.

This paper attempts to provide an overview of this dynamic field. It explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies, its characteristics, capabilities and the architecture of MANET. It also explains the IEEE standard 802.11 for Wireless LANs (WLANs) and all the circumventing design issues and how it can be used to enable ad hoc networking.

Keywords: Ad Hoc network, MANET, IEEE 802.11, MAC.

I. INTRODUCTION

During the last few years, Internet has become the major driving force behind most of the new developments in the telecommunication networks field. The volume of packet data traffic has been growing at a much faster rate than the telephone traffic. Meanwhile, there has been an exponential growth in the wireless field. The emergence of wireless communications and the increasing demand for mobility, distributed coordination and the ad hoc infrastructure brought in the foreground for ad hoc networks.

A Mobile Ad Hoc NETwork (MANET) is an autonomous system of mobile hosts (MHs) (also serving as routers) connected by wireless links and the union of which forms a communication network modeled in the form of an arbitrary communication graph. In a MANET, no infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. The mode of operation in ad hoc network is peer – to – peer multi – hop mobile wireless networks where information packets are transmitted in a store – and – forward manner from the source to an arbitrary destination. The Figure 1 below depicts Moblie Ad Hoc Network (MANET).

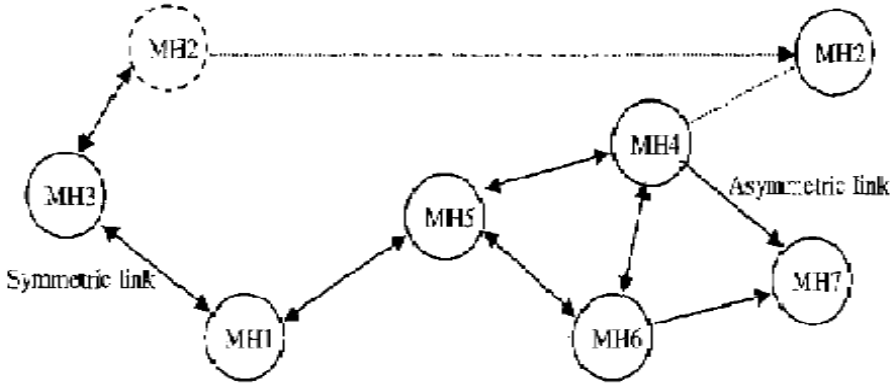

Figure 1 : A Mobile Ad Hoc Netwok (MANET)

A number of Wireless Ethernet standards have been developed and the two most common standards are IEEE 802.11 and ETSI HyperLAN [1]. Both the standards specify similar physical layers, but differ

significantly in their Medium Access Control (MAC) layers [2]. The IEEE 802.11 technology is a good platform to implement single – hop ad hoc networks because of its extreme simplicity. Single – hop means that the mobile hosts (MHs) must be within the same tranmission radius to be able to communicate. This limitation can be overcome by multi – hop ad hoc networking. This requires the addition of routing mechanisms at mobile hosts (MHs), so that they can forward packets towards the intended destination, thus extending the range of the ad hoc network beyond the transmission radius of the source mobile host (MH). Even though large – scale multi – hop ad hoc networks will not be available in the near future, on smaller – scales, mobile ad hoc networks are starting to appear thus extending the range of the IEEE 802.11 technology over multiple radio hops.

The multi – hop nature of ad hoc networks requires an appropriate protocol for the first and second OSI layers, so as to provide flexibiliity and robustness. There are several protocols to serve the above purpose. The choice of the most appropriate depends on each network's characteristics. Among all these, IEEE 802.11 is the most widely used in ad hoc networks, due to its functional maturity and its rapid commercial evolution. The characteristics of the wireless medium and the dynamic nature of the ad hoc networks make (IEEE 802.11) multi – hop networks fundamentally different from wired networks. Furthermore, the behavior of an ad hoc network that relies upon a carrier – sensing random access protocol, such as the IEEE 802.11, is further complicated by the presence of hidden stations, exposed stations, " capturing " phenomena [7, 22] and so on. The interactions between all these phenomena make the behavior of IEEE 802.11 ad hoc networks very complex to predict. Due to this fact, the performance of an IEEE 802.11 network is not stable and guaranteed.

This paper is organized as follows. Section II gives an overview of the Mobile Ad Hoc Networks in the evolution of wireless technologies, its characteristics and architecture. Section III describes the IEEE standard 802.11 for Wireless LANs (WLANs) and Section IV and V describes the IEEE 802.11 architecture, protocols and the main problems of IEEE 802.11 ad hoc networks. Section VI consists of the conclusions.

II. MOBILE AD HOC NETWORKS

Ad hoc networking capabilities can become essential in delivering overall next generation wireless network functionalities.

A. EVOLUTION OF MANETs

- In 1970, Norman Abramson and his fellow researchers at the University of Hawaii invented ALOHA net.
- In 1972, early ad hoc networking applications can be traced back to DARPA Packet Radio Network (PRNet) project [9], which was primarily inspired by the efficieny of the packet switching technology.
- In 1980, Survivable Radio Networks (SURAN) were developed by DARPA to address the main issues in PRNet, in the areas of network scalability, security, processing capability and energy management [8].
- During 1983, with the emergence of Internet Engineering Task Force (IETF) formed the mobile ad hoc networking group.
- In 1994, to leverage the global information infrastructure into the mobile wireless environment. Department of Defence (DoD) initiated DARPA Global Mobile (GloMo) Information Systems program, which aimed to support Ethernet – type multimedia connectivity anytime, anywhere among wireless devices [11].
- In 1995, the emergence of Bluetooth by Ericssion came into existence.

B. CHARACTERISTICS OF MANETs

- Dynamic Topologies
- Energy – constrained Operation
- Limited Bandwidth
- Security Threats
- Ease and Speed of Deployment
- Decreased Dependence on the Infrastructure
- Multi – Hop Network
- Each node working as an intelligent node
- No mediator networkingdevice is required for communication
- Each node works as a DTE (Data Terminal Eqipment) and DCE (Data Communication Equipment)

C. MANET ARCHITECTURE

This paper describes the ongoing research activities and the challenges in some of the main research areas within mobile ad hoc network domain. To present the research activities on ad hoc networks in a systematic and organic way, we describe as a reference, the simplified architecture of Mobile Ad Hoc Network (MANET) in Figure 2. The research activities are grouped according to a layered approach into three main areas :

- Enabling Technologies
- Networking
- Middleware and Applications

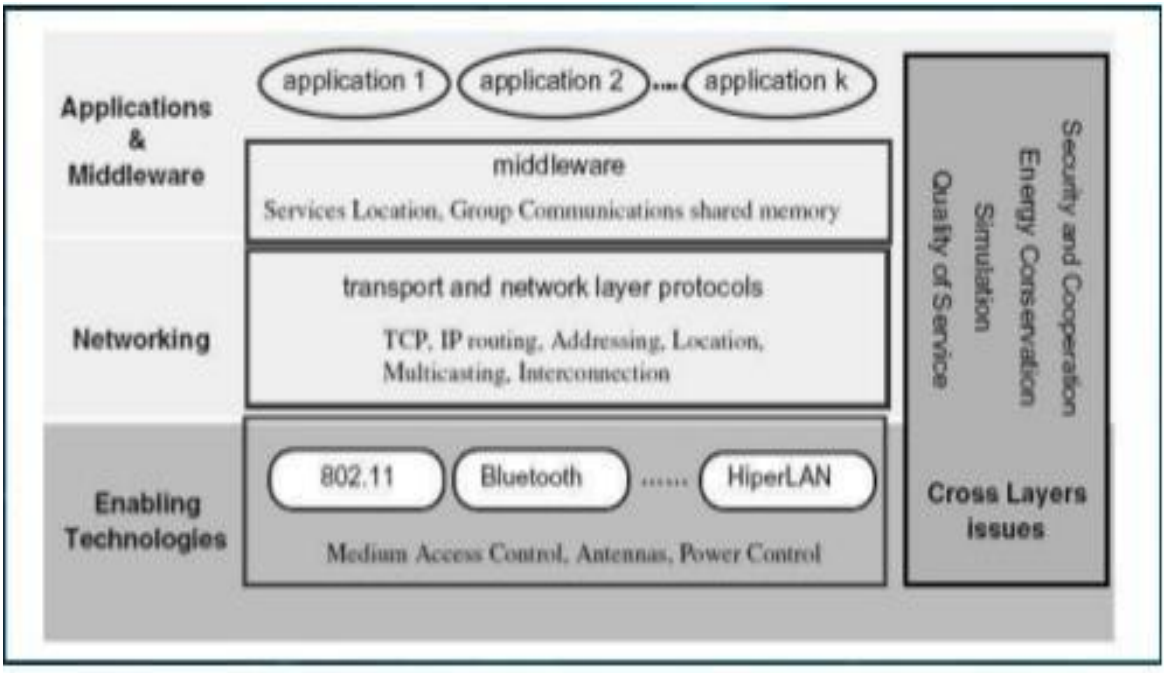

Figure 2 : MANET Architecture

1) Enabling Technologies

Ad hoc networks can be classified depending on their coverage area such as Body Area Network (BAN), Personalized Area Network (PAN), Local Area Network (LAN), Metropolital Area Network (MAN), Wide Area Network (WAN). BAN, PAN and LAN wireless technologies are already common in the market. These technologies constitute the building blocks for constructing small, multi – hop ad hoc networks that extend their range over multiple radio hops [11]. For these reasons, these technologies constitute the enabling technologies for ad hoc networking. Currently, two main standards are emerging for ad hoc wireless networks : IEEE 802.11 standard for Wireless LANs (WLANs) [12], and the Bluetooth specifications [13] for short range wireless communication [14, 15 and 16].

2) Networking

The aim of the networking protocols is to use the one – hop transmission services provided by the enabling technologies to construct an end – to – end (reliable) delivery services, from a sender to one (or more) receiver (s). Once, a user is located, routing and forwarding algorithms must be provided to route the information through the MANET. Finally, the low reliability of communications (due to wireless communications, user mobility etc.,) and the possibilty of network congestion requires a redesign of the Transport layer mechanisms.

3) Applications & Middleware

The introduction of new technologies such as the Bluetooth, IEEE 802.11 and HyperLAN greatly facilitates the deployment of ad hoc technology outside the military domain, and new ad hoc networking applications appeared mainly specialized fields such as emergency services, disaster recoveryand environment monitoring. In addition, MANET flexibility makes this technology attractive for several applicative scenarios

like, for example, in Personal Area Networking, home networking, law enforcement operation, search – and – rescue operations, commercial and educational applications, sensor networks [17].

III. IEEE 802.11 STANDARDS

Wireless LANs (WLANs) provide excellent usage model for high – bandwidth consumers, and they are quite appealing for their low infrastructure cost and high data rates as compared to other wireless data technologies such as cellular and point – to – multipoint distribution systems. In 1997, the IEEE adopted the first wireless local area network standard named IEEE 802.11, with data rates upto 2 Mbps. Since then, several task groups (designated by the letters from a, b, c, etc.,) have been creared to extend the IEEE 802.11 standard. Task groups 802.11b and 802.11a have completed their work by providing two relevant extensions to the original standard, which are often referred to with the name Wireless Fidility (Wi – Fi). There are three specifications for the 802.11 physical layers to operate in unlicensed radio bands.

IEEE 802.11a – This is a PHY layer standard for Wireless LANs (WLANs) in the 5 GHz radio band. It requires Orthogonal Frequency Division Multiplexing (OFDM) communication system. It specifies around 13 available radio channels, where the maximum link rate per channel is of 54 Mbps. Here, higher data throughput and greater number of channels give better protection against possible interference from neighboring access points.

IEEE 802.11b – This is a PHY layer standard for Wireless LANs (WLANs) in the 2.4 GHz radio band. It specifies three available radio channels, where the maximum link rate per channel is 11 Mbps. With increased usage, some installations may suffer from speed restrictions and have only three non – overlapping radio channels, which may cause interference from neighboring access points.

IEEE 802.11g – This is a PHY layer standard for Wireless LANs (WLANs) in the 2.4 GHz and 5 GHz radio bands and specifies three non – overlapping radio channels similar to 802.11b. The maximum link rate is 54 Mbps per channel as compared with 11Mbps for 802.11b. The 802.11g standard uses Orthogonal Frequency Division Multiplexing (OFDM) modulation, but for backward compatibility with 802.11b, it also supports CCK modulation and as an option for faster link rates allows packet binary convolution coding (PBCC) modualtion.

The performance of IEEE 802.11a, IEEE 802.11b and IEEE 802.11g can be considered with the following aspects:

1. Channels
2. Data Rate (Speed)
3. Frequency and Modulation Technique
4. Range and Density
5. Compatibility
6. Number of Users Per Access Point
7. Cost

1. Channels

802.11 systems divide the spectrum into differnet channels, so that Multiple Access Points can be set to each different channel. They operate closely without interference. However, 802.11b and 802.11g use overlapping channels, which means that out of the 11 channels used in the U.S, only the channels 1, 6 and 11 can be used effectively, allowing only three access points to operate without interference. In 802.11a, 12 access points can be operated in the same vicinity because it uses 12 channels that do not overlap.

2. Data Rate (Speed)

The data rate of IEEE 802.11a is 54 Mbps. The data rate of IEEE 802.11b is 11 Mbps. The data rate of IEEE 802.11g is 54 Mbps. Moreover, the data rate is distance dependent. As the distance increases, the data rate decreases.

3. Frequency and Modulation Technique

The frequencies of IEEE 802.11a, IEEE 802.11b and IEEE 802.11g are 5 GHz, 2.4 GHz and2.4 GHz respectively. Because of this reason, IEEE 802.11b and IEEE 802.11g can work in the same network without any problem. The modulation encoding techniques used for IEEE 802.11a is OFDM (Orthogonal Frequency Division Multiplexing), IEEE 802.11b is DSSS (Direct – Sequence Spread Spectrum) and CCK

(Complementary Code Keying), while IEEE 802.11g uses DSSS (Direct – Sequence Spread Spectrum) and PBCC (Packet Binary Convolution Code). The differences in the modulation encoding techniques make IEEE 802.11a incompatible with IEEE 802.11b and IEEE 802.11g networks. 802.11a and 802.11g use common 802.11 Medium Access Control (MAC) layer functions. As such, the protocols responsible for the operation of the network, including security, power management and fragmentation, are essentially the same. The IEEE standards 802.11a and 802.11g only implement the physical layer functions, such as modulation and demodulation, and not the higher layer functions.

4. Range and Density Comparison

The range of IEEE 802.11g is greater than IEEE 802.11a and almost same as that of IEEE 802.11b, but the density of IEEE 802.11g is much poor when compared to IEEE 802.11a and quite better than that of IEEE 802.11b. Thus IEEE 802.11g is much preferred where the range coverage is a hard issue and environment is less populated (i.e., the density is not an issue).

5. Compatibility

IEEE 802.11b and IEEE 802.11g are both compatible with each other because of two reasons. First, both use the same frequency band i.e. 2.4 GHz and same frequency modulation encoding technique i.e., DSSS (Direct – Sequence Spread Spectrum), although IEEE 802.11b also uses CKK (Complementary Code Keying) and IEEE 802.11g also uses PBCC (Packet Binary Convolution Code). As such, IEEE 802.11g and IEEE 802.11b are compatible to each other. That's why, the customers who donot wish to send data frequently (where speed is not a issue), are using IEEE 802.11b and are not upgrading their systems to IEEE 802.11g.

As the data rate of IEEE 802.11g is 54 Mbps and data rate of IEEE 802.11b is 11 Mbps, hence, it causes IEEE 802.11g device to reduce the data rate to effectively the same rates used by IEEE 802.11b. IEEE 802.11a and IEEE 802.11g use common IEEE 802.11 Medium Access Control (MAC) layer functions. As a result, the protocols responsible for the operation of the network; include security, power management and fragmentation are essentially the same.

The compatibility chart of IEEE 802.11a, IEEE 802.11b and IEEE 802.11g is shown in the Table 1 below.

Physical Layer Protocol	**IEEE 802.11a**	**IEEE 802.11b**	**IEEE 802.11g**
IEEE 802.11a	Yes	No	No
IEEE 802.11b	No	Yes	Yes
IEEE 802.11g	No	Yes	Yes

Table 1 : Compatibility Chart

6. Number of Users Per Access Point

IEEE 802.11a supports 64 users per access point. IEEE 802.11b supports 32 users per access point and IEEE 802.11g also supports 64 users per access point. But as the range of IEEE 802.11b is more as compared to that of IEEE 802.11a and IEEE 802.11g, that's why in a particular " cell ", IEEE 802.11b supports more number of users as compared to that of IEEE 802.11a and IEEE 802.11g. IEEE 802.11b (often called Wi – Fi) has the ability to serve upto four to five times more number of users than they now do. It also opens the possibility for using IEEE 802.11 networks in more demanding applications, such as wireless multimedia video transmission and broadcasting MPEG.

7. Cost

IEEE 802.11a is costly. IEEE 802.11b is of low price. But, if we compare IEEE 802.11a and IEEE 802.11b with IEEE 802.11g, we find that IEEE 802.11g is less expensive than IEEE 802.11a but expensive than IEEE 802.11b. The appliances of IEEE 802.11g may interfere on the unregulated signal frequency.

Comparison between IEEE 802.11a, IEEE 802.11b and IEEE 802.11g is shown in Table 2 below.

	IEEE 802.11a	**IEEE 802.11b**	**IEEE 802.11g**
Standard Ratified	September 1999	September 1999	May 2003
Raw Data Rates	54 Mbps	11 Mbps	54 Mbps
Average Actual Throughput	4 – 5 Mbps	27 Mbps	20 – 25 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz
Available Spectrum	300 MHz	83.5 MHz	83.5 MHz
Modulation Encoding	OFDM	DSSS / CCK	DSSS / PBCC
Number of Channels / Non – overlapping	12 / 8	11 / 3	11 / 3

Table 2 – Comparion between IEEE 802.11a, IEEE 802.11b and IEEE 802.11g

IV. IEEE 802.11 ARCHITECTURE AND PROTOCOLS

This section focuses on IEEE 802.11 architecture and protocols as defined in the original standard [3], with particular attention to the Medium Access Control (MAC) layer. The IEEE 802.11 standard specifies both the Medium Access Control (MAC) layer and the Physical layer (see. Figure 3). IEEE 802.11 is currently the most mature technology for infrastructure – based Wireless LANs (WLANs). The IEEE 802.11 standard defines two operational modes for Wireless LANs (WLANs) :

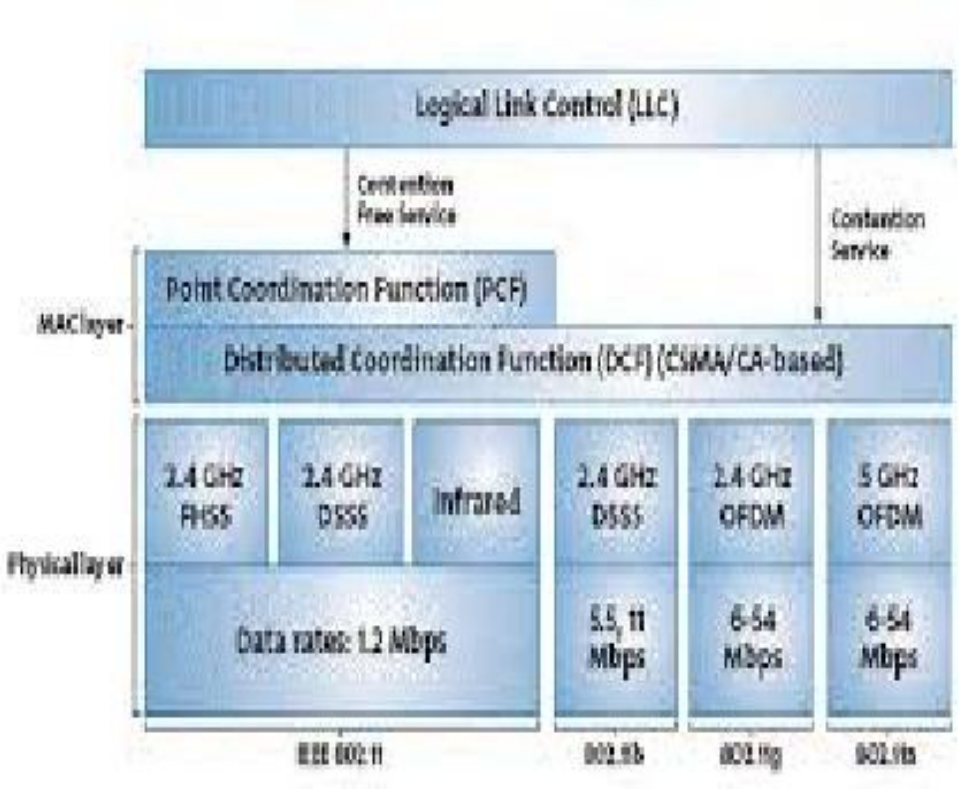

Figure 3 : IEEE 802.11 Architecture

- Infrastructure – Based
- Infrastructure – less or Ad hoc

The Point Coordination Function (PCF) is used in infrastructure networks, where an Access Point (AP) is used to co – ordinate access to the radio spectrum. Of more interest to ad hoc networks is the Distributed Coordination Function (DCF) which is used when there is no Access Point (AP) available, and individual 802.11 nodes must contend with each other for access to the media in a distributed fashion. Network interface cards can be set to work in either of these modes but not in both simultaneously. The infrastructure – based is the mode commonly used to construct the so – called Wi – Fi hotspots, i.e., to provide wireless access to the Internet. The drawbacks of an infrastructure – based Wireless LANs (WLANs) are the costs associated with purchasing and installing the infrastructure. These costs may not be acceptable for dynamic environments in which people and / or vehicles need to be temporarily interconnected in areas without a preexisting communication infrastructure (e.g., inter – vehicular and disaster networks), or where the infrastructure cost is not justified (e.g., in – building networks, specific residential community networks, etc.). In these cases, a more efficient solution can be provided by the infrastructure – less or ad hoc mode.

The DCF provides the basic access methods of the 802.11 MAC protocol and is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA) scheme. The PCF is implemented on top of the DCF and is based on a polling scheme. It uses a Point Coordinator that cyclically polls stations, giving them the opportunity to transmit. Since the PCF cannot be adopted in the ad hoc mode, it will not be considered hereafter. According to DCF, before transmitting a data frame, a station must sense the channel to determine whether any other station is transmitting. If the medium is found to be idle for an interval longer than the Distributed Inter Frame Space (DIFS), the station continues with its transmission (shown in Figure 4 below).

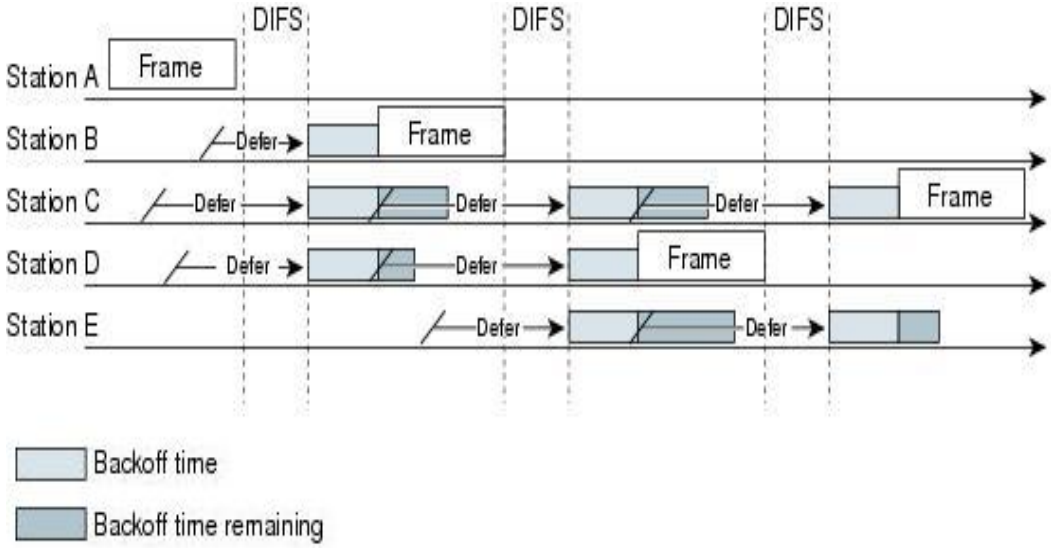

Figure 4 : Basic Access Mechanism

On the other hand, (i.e., if the medium is busy) the transmission is deferred until the end of the ongoing transmission. A random interval, referred to as backoff time, is then selected, which is used to initialize the backoff timer. The backoff timer is decreased for as long as the channel is sensed as idle, and the transmission stops when another transmission is detected on the channel. The transmission is reactivated when the channel is sensed idle again for more than a DIFS (Disributed Inter Frame Space). The stations are enabled to transmit its frame when the backoff timer reaches zero. The backoff time is slotted. Specifically, the backoff time is an integer number of slots uniformly chosen in the interval (0, CW – 1), where CW is defined as the Backoff Window and also referred to as Contention Window. At the first transmission attempt CW = CW_{min}, and it is doubled at each retransmission upto CW_{max}.

It may happen that two or more stations start transmitting simultaneously and a collision may occur. In the Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA) scheme, stations are not able to detect a collisionby hearing their own transmission (as in the CSMA / CD protocol used in Wired LANs). Therefore, an immediate positive acknowledgement scheme is employed to ascertain the successful reception of a frame. Specifically, upon reception of a data frame, the destination station initiates the transmission of an

acknowledgement frame (ACK) after a time interval called Short Inter Frame Space (SIFS). The SIFS (Short Inter Frame Space) is shorter than the DFIS (Distributed Inter Frame Space), in order to give priority to the receiving station over other possible stations waiting for transmission. Figure 5 shows that SIFS is shorter than DIFS.

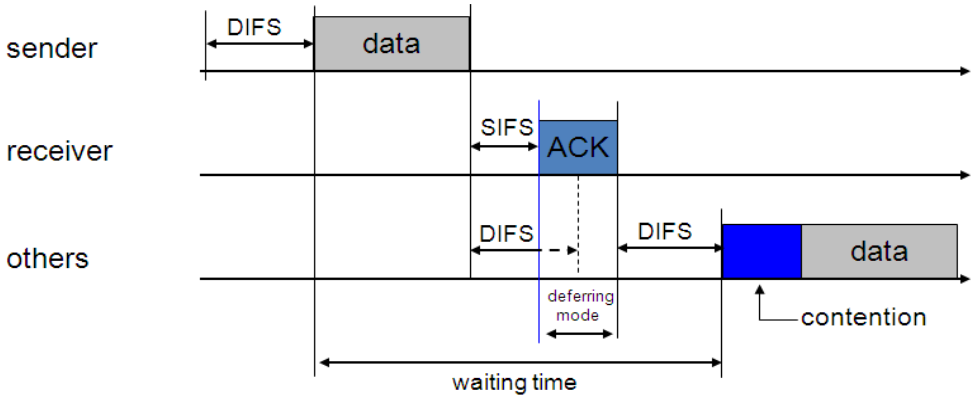

Figure 5 : Interaction between the Sender and Receiver showing SIFS is shorter than DIFS

If the ACK is not received by the source station, the data frame is presumed to have lost, and a retransmission is scheduled. The ACK is not transmitted if the received frame is corrupted. A Cyclic Redundancy Check (CRC) algorithm is used for error detection. After an erroneous frame is detected (due to collisions or transmission errors), a station must remain idle for atleast an Extended Inter Frame Space (EIFS) interval before if reactivates the backoff algorithm. Specifically, the EIFS shall not be used by the DCF whenever the physical layer has indicated to the MAC that a frame transmission was begun that did not result in the correct receptionof a complete MAC frame with a correct FCS value. Reception of an error – free frame during the EIFS re – synchronizes the station to the actual busy / idle state of the medium, so the EIFS is terminated and normal medium access (using DIFS and if necessary backoff) continues following reception of that frame.

V. MEDIUM ACCESS CONTROL PROTOCOL ISSUES

There are many issues that need to be addressed in order to design an efficient Medium Access Control protocol in a wireless ad hoc network environment [20]. Several MAC protocols can be employed for ad hoc networking such as IEEE 802.11 [19], Bluetooth [18], and HyperLAN. In this section, some fundamental issues that guide the design of MAC protocols for wireless networks are discussed.

A. Hidden Terminal Problem

A well known problematic side – effect of IEEE 802.11 MAC scheme is the hidden terminal problem [5] shown in Figure 6. The hidden node is one that is close enough to the receiver of a transmission such that it can interfere with a transmission being received, but far enough from the sender of that transmission such that the sender does not know the channel is re – busy at the receiver's location. This causes a collision at the receiver of both transmissions and a waste of network bandwidth.

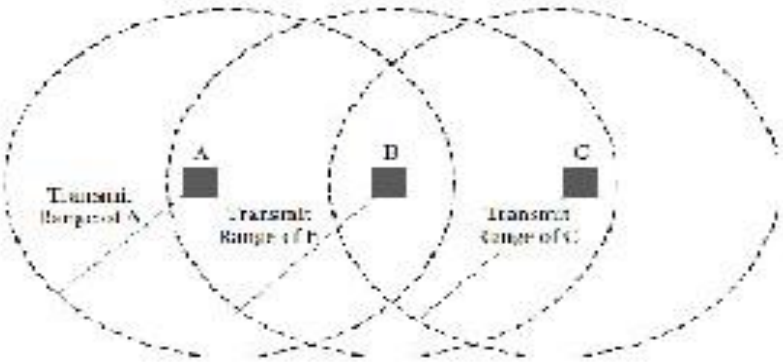

Figure 6 : The Hidden Terminal Problem.

In the Figure 6 shown above, Node A and Node C cannot sense each other transmissions (they are out of range of each other) and so other transmissions collide at Node B. A handshaking protocol is often used to deal with this problem [6]. A node wishing to make a transmission request uses an RTS (Request To Send) message. The receiving node then sends out a CTS (Clesr To Send) message, if it detects the medium as idle. A virtual carrier sense mechanism is employed by nodes via their Network Allocation Vector (NAV). Any node hearing either RTS or CTS message will update its NAV for a time period given in the RTS / CTS message, and refrain from transmitting during this period. The channel is then effectively reserved for the sender.

B. Exposed Node Problem

Exposed nodes [7] are those close enough to a transmitter to hear its transmission, and hence refrain from using the media, but far enough from the destination such that its own transmission would not interfere with the reception of the original message at that destination, due to the limited range of wireless transmissions. This leads to under utilization of the medium. The Figure 7 illustrates the Exposed Node Problem.

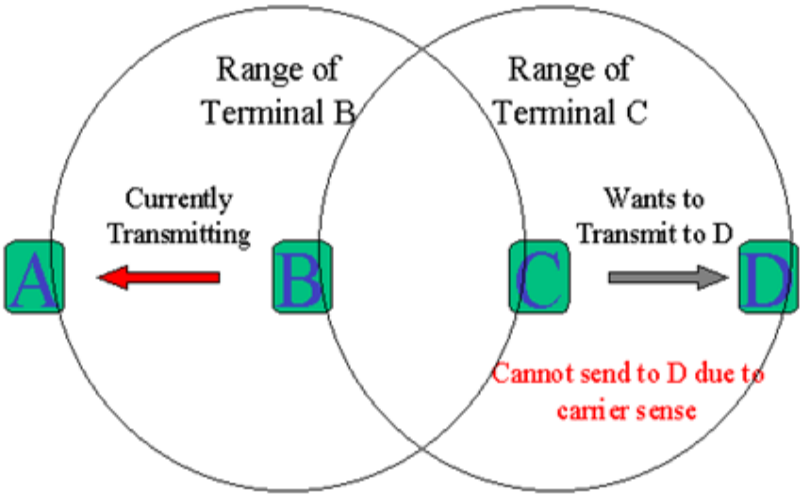

Figure 7 : Exposed Node Problem

Interference can cause packets to be incorrectly received at their destination. The 802.11 standard requires that nodes send explicit acknowledgements for unicast packets they receive [4]. If the sender does not receive the acknowledgement in a specified time frame, a number of automatic link – level retransmissions are performed for unicast packets. Broadcast packets, on the other hand, use neither positive acknowledgements nor virtual carrier sense mechanisms, and so loss rates of broadcast packets can be significantly higher than unicast packets.

VI. CONCLUSION

In the coming years, mobile computing will keep flourishing and an eventual seamless integration of MANET with other wireless networks and the fixed Internet infrastructure appears inevitable. The low cost of Wireless LANs has led to a tremendous growth of its worldwide use. Nowadays, we can find wireless LANs in nearly all enterprise environments, homes, hotspots, airport lounges, and among others. In the near future, the use of Wireless LANs will be as common as it is the use of cell phones nowadays.

Ad hoc networking is at the centre of evolution towards the 4^{th} generation wireless technology. Its intrinsic flexibility, ease of mainentance, lack of required infrastrucutre, auto – configuration, self – administration capabilities and significant costs are the advantages and makes it the primary candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community.

Finally, it can be stated that in the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad hoc Networks (MANETs). Hence, it becomes the best solution for different problems of the network.

REFERENCES

[1]. G. A. Halls, HIPERLAN : The high performance radio local area network standard, Electronics and Communication Engineering Journal, December, 1994

[2]. Angela Doufexi, Simon Armour, Peter Karlson, Andrew Nix, David Bull, A comparison of HIPERLAN / 2 and IEEE 802.11a, Centre for Communication Research, University of Bristol, UK Technical Report

[3]. IEEE standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, August 1999.

[4]. B. Crow, I. Widjaja, J. D. Kim and P. T. Sakai, IEEE : 802.11 : Wireless Local Area Networks, September 1997.

[5]. L. Klienrock and F. Tobagi, Packet Switching in Radio Channel, Part II – The Hidden Teminal Problem in Carrier Sense Multiple Access and the Busy Tone Solution, IEEE Transactions on Communications, Volume 23, pp. 1417 – 1433, 1975.

[6]. Phil Karn, MACA – A New Channel Access Method for Packet Radio, ARRL / CRRL Amateur Radio 9th Computer Networking Conference, 1990.

[7]. Shogong Xu and Tarek Saadwai, Does the IEEE 802.11 MAC Protocol Work Well in Multi – hop Wireless Ad Hoc Networks ?, IEEE Communications Magazine, pp. 130 – 137, June 2001.

[8]. W. Fifer, F. Bruno, The low – cost packet radio, Proceedings of the IEEE 75 (1), 1987, pp. 33 – 42.

[9]. James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks, in : Charles E. Perkins (Ed), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29 – 51.

[10]. B. Leiner, R. Ruth, A. R. Sastry, Goals and Challenges of the DARPA GloMo program, IEEE Personal Communications 3 (6), 1996, 34 – 43.

[11]. M. S. Corson, J. P. Maker, J. H. Cernicione, Internet – Based Mobile Ad Hoc Networking, IEEE Internet Computing 3 (4), 1999, pp. 63 – 70.

[12]. Mario Gerla, Jack Tsai, Multicluster Mobile Multimedia Radio Network, ACM / Baltzer Journal of Wireless Networks 1 (3), 1995, pp. 255 – 265.

[13]. Web site of the Bluetooth Special Interest Group : http://www.bluetooth.com/

[14]. C. Bisdikian, An Overview of the Bluetooth Wireless Technology, IEEE Communication Magazine, December 2001.

[15]. Specification of the Bluetooth System, Version 1.1, February 2001.

[16]. B. A. Miller, C. Bisdikian, Bluetooth Revealed, Printice Hall, Englewood Cliffs, NJ, 2000.

[17]. A. J. Goldsmith, S. B. Wicker, Design Challenges for Energy – Constrained Ad Hoc Wireless Networks, IEEE Wireless Communications 9 (4), 2002, pp. 8 – 27.

[18]. Bluetooth SIG, " Bluetooth Specification ", http://www.bluetooth.com.

[19]. IEEE Standard 802.11, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, June 1997.

[20]. E. M. Royer, S. J. Lee and C. E. Perkins, The Effects of MAC Protocols on Ad Hoc Communication Protocols, in Proceedings of IEEE WCNC 2000, September 2000.

[21]. S. Xu and T. Saadwai, Revealing the Problems with 802.11 MAC Protocol in Multi – Hop Wireless Networks, Computer Networks, Volume 38, March 2002.