IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 6 (Sep. - Oct. 2013), PP 84-88
www.iosrjournals.org

MAC Protocols: A Review

Shifali Hans
MTech, Central University Of Punjab, Bathinda, India

Abstract : *Mobile adhoc networks (MANETS) are infrastructureless networks which uses radio signals, to establish communication among mobile nodes. MANET media is open shared media, multiple mobile nodes may access the medium at the same time, which causes various MAC problems. This paper provides a review of various MAC problems being faced by MANETS and various MAC protocols which try to resolve these issues.*

Keyword: *MANETs, MAC, IEEE, Protocols, NCS.*

I. INTRODUCTION

Communication and information sharing is the most important strategic issue in today's era. With the advent of cheap portable devices and advances in the wireless technology [4], the wireless communication system took a stride. Spontaneous deployment of networks for better resource sharing is required in various fields like in military and rescue operations, virtual class room sessions, crisis management services, collaborative computing etc [1] [7]. This instant requirement has been furnished through Mobile Adhoc Network (MANETs). These networks have shown a revolutionary development as they are self configurable and self healable [4] [7].

Mobile adhoc networks are the networks, which consist of various mobile nodes that establish connection among themselves by using wireless medium i.e. radio signals [9]. The term "ad hoc" means that the network is established for a special, extemporaneous service [7]. They do not use any pre-existing infrastructure [6]. Because of this they can be deployment easily and therefore can be used in various applications. Nodes in MANETS intercommunicate either in single hop or through multihop manner [7] [9]. If the receiver node is in the transmission range of sender, node can communicate directly with other node i.e. single hop, and in case the node is not in the direct transmission, that is far away, in that case, packet has to be relayed through nodes that are in the path of sender and receiver, i.e. multihop. Nodes in MANETs act as host as well as router [7] [9].

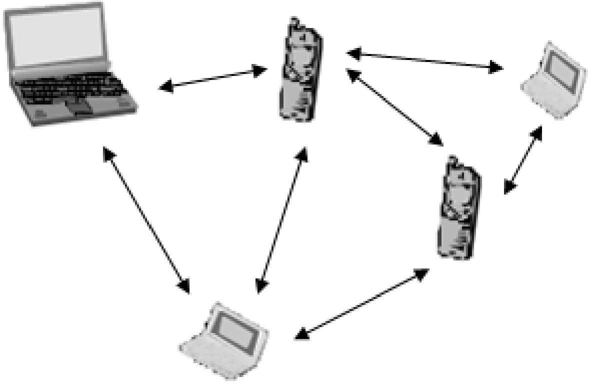

Figure 1. Mobile Adhoc Network

Communication in the MANETs is broken down into series of layer. Each layer has specific functions. This hierarchical structure is modeled in such a manner that each layer isolates the layer above it from the rest of the protocol stack. The benefit of this is that, as technology advances the lower layers can be replaced, without affecting the upper layers as long as the interface between layers remains constant[15] [16]. The hierarchy uses encapsulation to provide the abstraction of protocol and services [15]. Figure 2 shows the typical protocol stack of a network.

Application layer: This layer provides the interface and support service to the user. It encodes the data being sent and make sure that data format is understandable by the recipient. Various higher level protocols like HTTP, FTP, TFTP, TELNET, and SNTP operate at this layer [15].

Transport layer: This provides process to process interaction. It split the data into chunks called data packets and adds the packet number. Each packet contains the port number depending upon the application being used. TCP and UDP protocol operates at this layer [15].

Network layer: Also called as internet layer. This layer has the task of providing route to the datagrams. Various routing protocols like AODV, DSDV, TORA, etc. are used to route the datagrams. Protocols like ICMP, IP are also used at this layer.

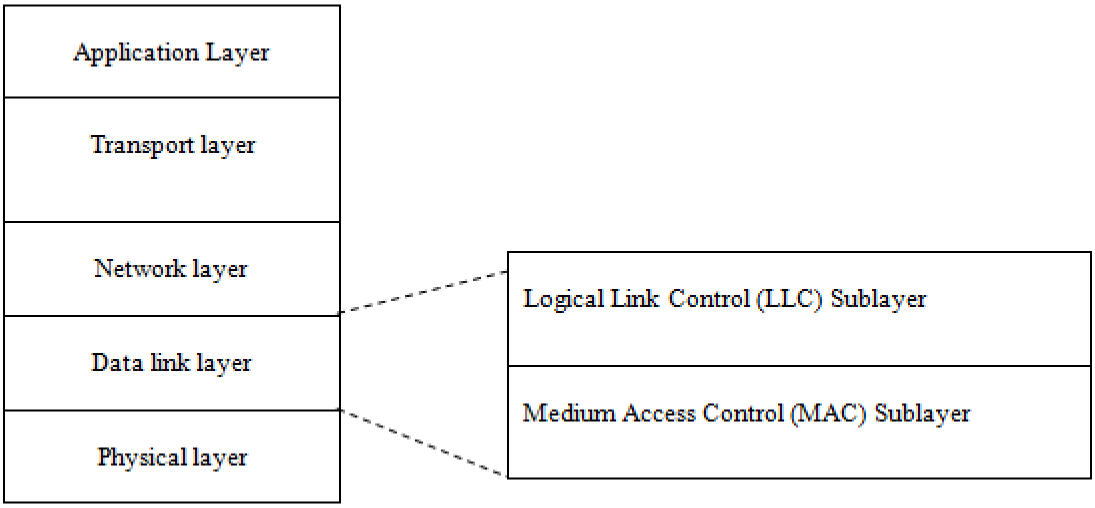

Figure 2. Protocol Stack

Data link layer: It attaches the MAC address of the sender and the recipient, allowing the packets to be directed to specific network interface on the IP Address host machine [15].

Physical layer: This is the lowest layer and consists of the basic networking hardware technologies [15]. It provides the procedural, mechanical and electrical interface to the transmission medium.

II. MAC SUBLAYER

Data link layer has two sublayer – LLC and MAC [9] [15]. Logical Link Control sublayer provides multiplexing mechanisms that help several other protocols to coexist. It also provides flow control and ARQ error management mechanisms [16].

MAC sublayer is the interface between the LLC and the physical layer. MAC contains the mechanism that regulates the channel access. MAC is like traffic guard which gives directions that how mobile node will access the medium with minimum packet collision and delay in transmission [9] [15]. MAC Protocols are the most important factor which determines the performance of a MANET [16].

To regulate the user access to medium is very crucial aspect of the MANETS. Radio medium is open shared medium [7], it not possible to have separate communication lines; this causes media access problems.

Problems at MAC layer:

Due to decentralized control and wireless channel characteristics, MAC faces hidden and exposed terminal problem [1].

Hidden Terminal Problem: The hidden terminal problem was first mentioned by Kleinrock and Tobagi. Hidden nodes are those nodes that are not in the range of sender but are in the range of receiver [2]. Due to these hidden nodes, collision of packets occurs at receiver. The probability of collision of packets is directly proportional to the number of terminals hidden from the sender [1] [9] [10].

To illustrate this hidden terminal problem, lets us take three nodes Sender (A), Destination (B), Hidden terminal(X). Now consider the transmission range of these nodes. Destination B is within the transmission range of A and X. A is in the transmission range of B but not X. X is in the transmission range of B but not in the transmission range of A. That means that both A and X is hidden from each other. Now, let A want to send some data packets to B. A will sense the medium and if it is free, it will send the packets to B. But, at the same time, suppose, X also want to send the packets to the B, he will also sense the medium, and will also find medium free (as A transmission is outside its range) [10] [12]. X will also start sending packets to B. But, this simultaneous transmission of packet by X will cause packet collision at B. This collision occurred because of hidden terminal X, which was in the range of B (receiver) but not in the range of A (sender).

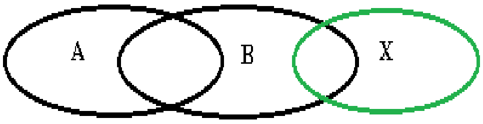

Figure 3. Hidden Terminal

Exposed Terminal Problem: Exposed terminal are those terminals that are within the range of sender, but are not in the range of receiver [2]. As these exposed terminals are within the range of sender, they face a delay in transmission to another node, due to the transmission of nearby node [9]. The probability of unsuccessful transmission is proportional to the number of exposed terminals [1] [10].

To illustrate this exposed terminal problem let us take nodes Sender (B), Destination (A), Exposed terminal(Y). Now consider the transmission range of these nodes. Destination B is within the transmission range of A and Y. A is in the transmission range of B but not Y. Y is in the transmission range of B and K but not in the transmission range of A. Now, suppose B is sending data packets to A. And the exposed terminal Y wants to send the data packet to another node (let it be K) which is outside the range of A and B, but is within the range of Y. So, Y will sense the medium and will find it busy (as communication is going between A and B) and will therefore postpone its transmission. But this delay is unnecessary as A is outside the interference range of Y. Collision at B does not matter as the collision is too weak to propagate to A. In this case, Y is exposed to B [10] [12].

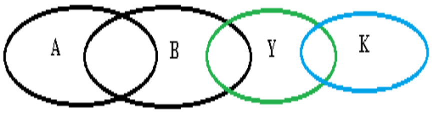

Figure 4. Exposed Terminal

The hidden and exposed terminal problem is more pronounced in wireless networks. The collision of packet and unsuccessful transmission severely affect the performance of higher layer schemes like network congestion and routing maintenance [3]. MAC schemes for wired networks (CSMA/CD) often get fail in wireless networks because in wireless strength of the signal decreases proportionally with the square of distance [7] [9] [12]. So, there was the need for specialised MAC protocol for wireless networks [9] [12].

III. MAC PROTOCOLS

A MAC protocol plays a crucial role in determining the throughput, efficiency, delay, energy efficiency of a network [3]. The various MAC protocols which help in mitigating the hidden and exposed terminal effect are discussed below:

BTMA (Busy Tone Multiple Access): It was the first protocol to combat the hidden terminal problem of Mobile adhoc network. The transmission channel is divided into – one for the data and other for the busy tone signal. When a node wants to transmit data to another node, it firstly senses the medium and check whether the busy tone is active. If it is active it will wait for some random time and then will retry. If busy tone is inactive, it will turn on the busy tone signal and sends the data. The limitation of BTMA is that it uses the different channel to show the busyness [17][18].

SRMA (Split Channel Multiple Access): The first protocol that was based on the RTS/CTS handshake mechanism was SRMA. In SRMA, the sender by using ALOHA or CSMA decide when to sends the RTS (ready-to-send) to the destination. And, the destination response back by the CTS (clear-to-send), which tell the sender, when to start the transmission [17][18].

MACA (Multiple Access with Collision Avoidance): This protocol was proposed by Karn. It uses three way handshake i.e RTS-CTS-DATA. RTS (ready-to-send) and CTS (Clear-to-send) are two short signaling packets. If a node A wants to transmit to node B, it first sends an RTS (ready-to-send) packet to B, RTS will also indicate the length of the data transmission that would later follow. If B receives this RTS packet, it returns CTS (Clear-to-send) packet to A, CTS will also contains the expected length of the data to be transmitted. When A receives the CTS, it immediately commences transmission of the actual data to B. The key idea of the MACA scheme is that any neighboring node that overhears a CTS packet has to defer its own transmissions, until the data transmission is complete [8] [12].

In a hidden terminal scenario, X will not hear the RTS sent by A, but it would hear the CTS sent by B. Accordingly, C will defer its transmission during A's data transmission. Similarly, in the exposed terminal situation, Y would hear the RTS sent by B, but not the CTS sent by A. Therefore, C will consider itself free to transmit during B's transmission. MACA is as RTS and CTS packets are significantly shorter than the actual data packets, and therefore collisions among them are less expensive compared to collisions among the longer data packets [12].

MACAW(Multiple Access with collision Avoidance for wireless): In order to overcome the weaknesses of MACA, Bharghavan proposed MACA for Wireless (MACAW) scheme that uses a five step RTS–CTS–DS–DATA–ACK exchange [6][8][12].

Suppose node A has to send data to node B. Node A initiates the process by sending a RTS (Request to Send) frame to node B. The destination node (node B) replies with a CTS (Clear to send) frame. After receiving CTS, node A sends data. After successful reception, node B replies with an acknowledgement frame (ACK). Before sending a long DATA frame, node A sends a short Data Sending frame (DS), which provides information about the length of the DATA frame. Any node (node C) overhearing a CTS frame refrains from sending data to B, until the transmission between A and B is complete. Both the RTS and CTS frames contain information about the length of the DATA frame. Hence a node uses that information to estimate the time for the data transmission completion [9].

The use of acknowledgment packet (ACK) in MACAW provides better error recovery at the data link layer. The acknowledgment packets are returned from the receiver to the sender when the data reception is completed. MACAW achieves significantly better throughput as compared to MACA. However, it could not fully solve the hidden and exposed terminal problems of MANETs [12].

FAMA-NCS (Floor acquisition multiple access-Non Persistent Carrier): FAMA-NCS is the single channel protocol that guarantees that a single sender is able to send the data packets to the receiver without any collision [8]. FAMA provide collision avoidance both at the sender as well at the receiver. It allows the transmitting station to acquire the control of floor (channel) [8]. In order to acquire the floor FAMA uses three way handshake RTS/CTS/DATA. Sender uses non- persistent carrier sensing to send RTS to the receiver. And, if the receiver is free, it sends the CTS to the sender, the CTS of the receiver lasts much longer than the RTS of the sender which serve as the 'busy tone'. This busy tone forces the hidden nodes to back off, thus allowing the collision free data to arrive at receiver [12].

DBTMA (Dual Busy tone Multiple Access): This protocol is the extension of the BTMA scheme [4]. Two channels are used. One is data channel and other control channel. Data channel is for the data packet transmissions, and a control channel is used for control packet transmissions (RTS and CTS packets) and also for transmitting the busy tones. RTS packet is used to initiate channel request. Two busy tones are used to protect the RTS and CTS. One of the busy tones is set by the sender and is used to protect the RTS packet. And another busy tone set by the receiver is used to protect the CTS of the receiver and to provide the protection for the incoming data packets. Other nodes in the vicinity that overhears any of these busy tones defer their transmission [4] [8].

DE-FACTO MAC PRTOCOL IEEE 802.11 DCF:

IEEE adopted first wireless LAN standard, IEEE 802.11, in 1997. Since then various extensions of IEEE 802.11 have developed. IEEE 802.11 has two modes – PCF and DCF. PCF (Point coordination function) is for the infrastructure network while DCF (Distributed coordination function) is for the adhoc networks [6]. It is basically a combination of CSMA/CA and MACA [12]. It performs physical carrier sensing as like CSMA and also virtual carrier sensing by using NAV (Network allocation vector) [11]. NAV is a timer which is maintained by every node that will be affected by the transmission [12] [13].

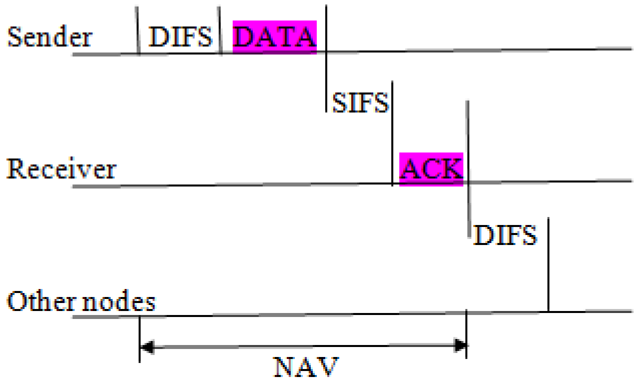

Figure 5. IEEE 802.11 DCF

IEEE 802.11 DCF uses four way handshake i.e. RTS/CTS/DATA/ACK. RTS and CTS are two short control messages that resolve the data packet collision. A node before sending the data packet senses the medium, if the destination node is busy, it will back off for certain time period. And, in case it is idle sender will send the RTS. On receiving the RTS, the destination node will send the CTS, this will indicate that destination is ready to receive the data. Sender will then send the data packet. Finally the destination will send the acknowledgement to the sender that it has successfully received the data. RTS usually include the duration of the time for which node will be busy. So the other node in the vicinity set the NAV accordingly. NAV represents that how much time must pass before checking the channel for idleness and this will eventually avoid the collision from the hidden nodes [11][13][14][16].

There are several issues concerning IEEE 802.11that are not addressed. IEEE 802.11 do not consider the QoS nor the fairness issues. Moreover, an effective transmission scheme based on the channel condition is still open and challenging. MAC contention often introduces network congestion with backlogged packets Carrier sensing strategy based on RTS/CTS often result in low spatial reuse [2].

Furthermore, NAV setup introduces some serious limitations. NAV cannot work efficiently when there is collision among RTS/CTS/DATA/ACK. These packets can become corrupt due to collision [2]. For example, in Fig 4, B wants to send packets to Y. They exchange RTS and CTS. If K is transmitting when Y transmits CTS to B, Y's CTS and K's transmission may collide, and A will set its NAV according to the corrupted CTS from Y [2]. Also, if a node is continuously doing carrier sensing, and there are multiple communications going simultaneous NAV setup become redundant [2].

IV. CONCLUSION

Mobile Adhoc Networks provide ubiquitous networking. They can be deployed easily anywhere anytime. But these MANETs are facing various problems. MAC layer collision in MANETs is much more severe than expected. The MAC protocol that can efficiently avoid collision and error of packet, and provide better service is the need of hour. There are various MAC protocols that have been developed like BTMA, MACA, MACAW, IEEE 802.11 DCF, etc. But, still their efficiency is not up to the mark.

Moreover, due to MAC layer contention, the interaction among different traffic flows requires attention. It has been observed that MAC contention introduces network congestion. So, the MAC layer interaction with other higher layer protocols becomes a very crucial aspect of MANETs. MANETs are still in their adolescence and there are many more things to be explored and unveiled about MANETs.

REFERENCES

[1] A. Jayasuriya, S. Perreau, A. Dadej, S. Gordon, "Hidden vs. Exposed Terminal Problem in Ad hoc Networks*", Institute for Telecommunications Research,* Australian Telecommunication Networks & Applications Conference(ATNAC), pp 52-59, 2004

[2] H. Zhai and Y. Fang, "Medium Access Control Protocols in Mobile Ad Hoc Networks: Problems and Solutions", *Department of Electrical and Computer Engineering University of Florida*,http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.7011&rep=rep1&type=pdf, last accessed on 24 July 2013

[3] C. Huang, Chin-Tau Lea, Albert Kai-Sun Wong, "A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks" *Computer Networks*, *vol 56, Issue 14*, *pp. 3261-3273, 28 September 2012*

[4] H Zhai, J Wang, X Chen and Y Fang, "Medium access control in mobile ad hoc networks: challenges and solutions", *Wireless Communications And Mobile Computing*, pp. 151-170, 2006

[5] Chun-cheng Chen and Haiyun Luo, "The Case for Heterogeneous Wireless MACs", *Proceedings of HotNets*, 2004

[6] I. Chlamtac , Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", Adhoc networks, vol. 1, issue 1, pp. 13-64, July 2003

[7] P. Mohapatra, S. Krishanmurthy, "Adhoc networks technology and protocols", Springer, 2005, http://csis.bits-pilani.ac.in/faculty/murali/aos8/papers/Ad.Hoc.Networks.Technologies.And.Protocols. Sep. 2004.Springer.Verlag.Telos.eBook-DDU.pdf, accessed on 25 May 2013

[8] Z. J. Haas, and J. Deng, "Dual busy tone multiple access (DBTMA)-a multiple access control scheme for ad hoc networks." *Communications, IEEE Transactions, vol.* 50, no. 6, pp. 975-985, 2002

[9] J. Schiller, " Mobile Communications", Second Edition, Pearson Education,2003

[10] Viral V. Kapadia, Sudarshan N. Patel and Rutvij H. Jhaveri, "Comparative Study Of Hidden Node Problem And Solution Using Different Techniques And Protocols", *Journal Of Computing*, https://sites.google.com/site/journalofcomputing/ Vol 2, Issue 3, March 2010

[11] Anucha U. Sylvester, Asagba O. Prince, Ogheneovo E. Edward, "Carrier Sensing Mechanisms: The Impact On Throughput Performance Of IEEE 802.11 WLANs", *IJAR-CSIT*, vol 1, issue 1, 2012

[12] S. Kumar , V. S. Raghavan, J. Deng , Medium Access Control protocols for ad hoc wireless networks: a survey, *Science direct Ad Hoc Networks* , pp. 1-32, 2004

[13] Chaudet, D. Dhoutaut, I. Lassous, "Performance issues with IEEE 802.11 in ad hoc networking", *IEEE communication Magazine*, vol 43, issue 7, pp. 110-116, 2005

[14] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", *IEEE Journal On Selected Areas In Communications*, Vol. 18, No. 3, pp. 535-547 March 2000

[15] L. Litwin, "Medium Control Sublayer", Communication Technology, *IEEE Potentials*, vol. 17, no. 1, pp. 30-34, 2001

[16] Anastasi, Giuseppe, Eleonora Borgia, Marco Conti, and Enrico Gregori. "IEEE 802.11 ad hoc networks: performance measurements.". *23rd International Conference on Distributed Computing Systems*, 2003. Proceedings, pp. 758-763. IEEE, 2003.

[17] J.J. Garcia, Luna, Acevesy and Chane L. Fullmer, "Performance of Floor Acquisition Multiple Access in Ad-Hoc Networks" , *Third IEEE Symposium on_ Computers and Communications*, pp. 63-68, 1998

[18] R. Jurdak, C.V. Lopes, and P. Baldi, "A Survey, Classification and Comparative analysis of Medium access control protocols for Adhoc networks", *IEEE Communications survey and Tutorials*, vol 6, no. 1, 2004