IJCSN International Journal of Computer Science and Network, Volume 5, Issue 1, February 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Analyzing MAC Protocol for Wireless Ad-hoc Networks

[1] Gopal Singh Bhadoriya, [2] Reena Chauhan

[1,2] Department of Computer Science, ITM University, Gwalior, M.P., India

Abstract - Ad-hoc wireless networks are one of the fastest growing technology in the today's world. It is a collection of nodes which dynamically form a temporary network without any infrastructure. Medium Access Control(MAC) protocols are responsible for coordinating the access from active nodes in this network. MAC protocols are very importance for the wireless communication channel is inherently prone to errors and some problems such as hidden terminal problem and exposed terminal problem. Although a lot of researcher has been conducted on MAC protocols, the various issues involved have mostly been presented in isolation of each other. so, in this survey paper we present a classification of MAC protocols and their brief dicription, based on their operating principles and underlying features.

Keywords - *Ad-hoc Network, Issues, MAC Protocols, Security.*

1. Introduction

Ad-hoc networks are comprised of mobile nodes that exchange packets by broadcast radio channel. Due to the limitations of this channel, the bandwidth to be shared among the nodes is limited. Therefore, the aim in these networks is to be able to utilize the bandwidth efficiently, and guarantee fairness to all nodes. As we know, wireless networks differ enormously from wired networks; furthermore, ad hoc wireless networks have even more specific characteristics, such as node mobility, power constraints. Thus, new protocols are needed for controlling access to the physical medium. The unique properties of the ad hoc networks make the design of a media access control (MAC) protocol more challenging. This paper sets on giving a brief outline of the MAC protocols for ad hoc networks, focusing on contention-based algorithms with reservation and scheduling.

2. Design Issues

Following are the main issues one should have in mind when considering designing a MAC protocol for ad hoc wireless networks.

2.1 Bandwidth Efficiency

The scarcity of bandwidth resources in these networks calls for its efficient usage. To quantify this, we could say that bandwidth efficiency is the ratio of the bandwidth utilized for data transmission to the total available bandwidth. In these terms, the target will be to maximize this value.

2.2 Quality of Service Support

Providing QoS in these networks is very difficult, due to the high mobility of the nodes comprising them. Once a node moves out of another node's reach, the reservation in it is lost.

On the other hand, in these networks QoS is sometimes extremely important, for example in military environments. Therefore, QoS should be provided somehow, despite the characteristics of ad hoc networks.

2.3 Synchronization

Some mechanism has to be found in order to provide synchronization among the nodes. Synchronization is important for regulating the bandwidth.

2.4 Hidden and Exposed Terminal Problems

The reason for these two problems is the broadcast nature of the radio channel, namely, all the nodes within a node's transmission range receive its transmission.

2.5 Hidden Terminal Problem

Two nodes that are outside each-other's range perform simultaneous transmission to a node that is within the range of each of them, hence, there is a packet collision[1].

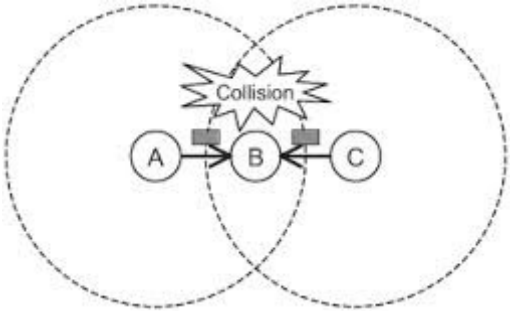

Figure 2.5: hidden terminal problem

2.6 Exposed Terminal Problem

The node is within the range of a node that is transmitting, and it cannot transmit to any node.

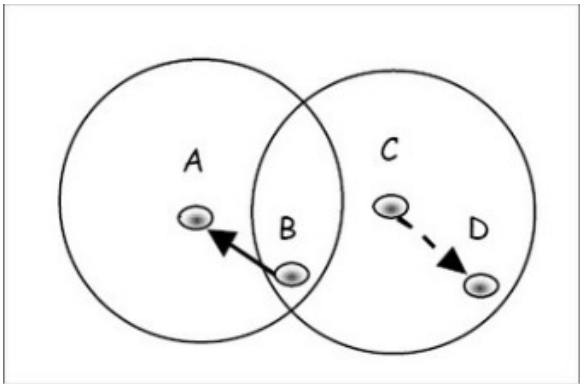

Figure 2.6: exposed terminal problem.

Hidden nodes mean increased probability of collision at a receiver, whereas exposed nodes may be denied channel access unnecessarily, which means underutilization of the bandwidth resources.

2.7. No Central Coordination

In ad hoc networks, there is no central point of coordination due to the mobility of the nodes. Therefore, the control of the access to the channel must be distributed among them. In order for this to be coordinated, the nodes must exchange information. It is the responsibility of the MAC protocol to make sure this overhead is not a burden for the scarce bandwidth.

2.8. Mobility of Nodes

The mobility of the nodes is one of its key features. The QoS reservations or the exchanged information might become useless, due to node mobility. The MAC protocol must be such that mobility has as little influence as possible on the performance of the whole network.

3. Literature Reviews

Classification of MAC protocol for ad hoc networks

Several criteria can be used for the classification of MAC protocols, such as time synchronization, initiation approach, and reservation approach. Ad hoc network protocols can be classified into three basic types-
Contention-based protocols
Contention-based

Contention-based protocols with scheduling mechanisms.

There are also some MAC protocols outside the above categories.

3.1 General Definition of Contention-Based Protocols

Here, the channel access policy is based on competition. Whenever a node needs to send a packet, it tries to get access to the channel. These protocols cannot provide QoS, since access to the network cannot be guaranteed beforehand.

3.2. General Definition of Contention-Based Protocols with Reservation Mechanisms

Protocols provide bandwidth reservation ahead; therefore, they can provide QoS support. These can be further subdivided into Synchronous protocols: there is time synchronization among all nodes in the network, the nodes in the neighborhood are informed of the reservations; Asynchronous protocols: no global synchronization is needed. Relative time is used for the reservations.

3.3 General Definition of Contention-Based Protocols with Scheduling Mechanisms

There can be packet scheduling at the nodes, or node scheduling for access to the channel. Node scheduling should not treat the nodes.

4. Ad hoc MAC Protocols

There are basically two main categories of MAC protocols: first is Random Access Protocols and second is controlled Access Protocols. Random Access Protocol specifies of detect collision or recover from collision.. In Controlled Access Protocols node decides which node get access to the medium. Peer-to peer nature and the lack of infrastructure ad hoc networking make Random Access Protocols the natural choice for medium access control in

ad hoc networks. Thus most ad hoc MAC protocols are based on the random access paradigm. Example includes MACA (Multiple Access with Collision Avoidance), MACAW (MACA with Acknowledgment), MACA-BI (MACA by Invitation), DBTMA (Dual Busy Tone Multiple Access) [2] and FAMA (Floor Acquisition Multiple Access). Amongst these protocols CSMA (Carrier Sense Multiple Access) protocols are those in which nodes, before transmitting, first listen for a carrier (i.e. , transmission) on the channel, and make decisions on whether or not to transmit based on the absence or presence of the carrier [3]. MAC Controlled Access Protocols example TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access), CDMA (Code Division Multiple Access) and TSMA (Time Spread Multiple Access) though seldom used in wireless ad-hoc networks are preferred in atmosphere that needs of Quality of Service (QOS) guaranteed as their transmissions are collisions free. Bluetooth and cluster-based ad hoc networks are their applications, where access to the shared medium is control by Master nodes [8].

Ad hoc MAC protocols include algorithms to reduce mobile stations energy consumption, like allowing stations to sleep during idle period and in the incorporation of directional antenna for improve the performance. Typically ad hoc network stations assume the use of omni-directional antennas. With omni-directional antennas, while two stations are communicating use a given channel, the MAC protocol requires that all other stations in the vicinity stay silent. But with directional antennas, two pairs of stations located in each other's vicinity may potentially simultaneously access the channel, depending on the directions of transmission. Directional antennas can adaptively select radio signals of interest in specific directions, while filtering out unwanted interference from other directions. This can increase spatial reuse of the wireless channel, in addition to higher power gain.

5. Security

The broadcast nature of ad hoc networks expose it to security attacks for performing communication in free space . Ad hoc wireless links are susceptible to attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Active attacks might allow the adversary to delete messages, inject erroneous, modify messages and impersonate a node, thereby violating authentication, availability, integrity, and nonrepudiation [9]. First step towards developing good security solutions understanding possible form of attacks. Preventive and detective two types of security mechanism can be generally applied. Preventive mechanisms are typically based on key-based cryptography. However, designing secure key distribution that allows the creation of unforgettable credentials in ad hoc networks is a challenging problem. Deffie–Hellman key exchange may indeed help to establish some temporary security between particular endpoints. However, they are also vulnerable to the man-in-the-middle attacks. The major security threats that exist in ad hoc wireless net work are as follows:

5.1 Denial of Service

The attack affected by making network resource unavailable for suitable in resource-constrained ad-hoc wirelss network.

5.2 Interference

It is a common attack and defense applications noise This can be done by using a single wide-band jammer, sweeping across the service to other node, either by consuming the bandwidth or by overloading the system, is known as denial of service (DoS).

5.3 Resource Consumption

The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resource available in the network.

5.4 Host Impersonation

A compromised internal node can act as another node and respond with appropriate control packets to create wrong route entries, and can terminate the traffic meant for the intended destination node.

5.5 Information Disclosure

A compromised node can act as an informer by deliberate discloser of confidential information to unauthorized nodes. Information such as the amount and the periodicity of traffic between a selected pair of nodes and pattern of traffic changes can be very valuable for military applications. The use of filler traffic (traffic generated for the sole purpose of changing the traffic pattern) may not be spectrum. The MAC and the physically technologies should be able to handle such as external threat.

6. Conclusion

Mobile Ad-hoc network is a current investigation topic. For efficient MAC protocol many investigations have been done. In this paper we have tried to survey MAC protocol mainly from a technical point of view. This paper provides

the fastest study of MAC protocol with various research issues. These issues may be used for further research work for improving the network's performance.

References

[1] L. Kleinrock and F.A. Tobagi, "Packetitching in radio channels: Part II - The hidden terminal problem in carrier sense multiple-access and the busy-tone solution," IEEE Trans. Commun. vol. COM-23. pp. 1417-1433, December 1975

[2] Z.J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA) - A multiple access control scheme for ad hoc networks," IEEE Transactions on Communications, vol. 50, no. 6, June 2002

[3] N. Jain, S.R. Das, and A. Nasipuri, "A multichannel CSMA MAC protocol with receiver-based channel selection for multihop wireless networks," in Proceedings of the Tenth International Conference on Computer Communications and Networks, 200

[4] Z. Tang and J.J. Garcia-Luna-Aceves, "Collision-avoidance transmission scheduling for ad-hoc networks," IEEE, 2000, pp. 1788-1794

[5] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocols for wireless sensor networks," in Proceedings of the IEEE Infocom 2002, New York, NY, June 2002, pp. 1567-1576

[6] P.J.M. Havinga, "EMACs - EYES MAC protocol for sensor networks," 7th Wireless World Research Forum, December 2002

[7] Shivani rao, Sanjeev khambra "A comparative analysis of MAC protocols in MANET" (IJETAE-2013).

[8] Prof. Neeraj agarwal, Dr. Sanjeev Sharma, Prof. Arun Nahar "Analysis of CSMA, MACA & EMACA(Enhancement of Multiple Accesses with Collision Avoidance) to Support QoS under varying conditions of No. of Nodes in Ad-Hoc Wireless Networks by means of DSR Routing Protocol" (IJCA-2010).

[9] C.Siva Ram Murthy and B.S Manoj, Mobile Ad Hoc Networks- Architectures & Protocols , Pearson Education,

[10] R. Hekmat and P. Van Mieghem, "Interference in Wireless Multi-hop Ad-hoc Networks and its Effect on Network Capacity," Wireless Networks Journal, Special Issue on Ad-hoc Networking, February 2003.

[11] LAN MAN Standards Commitee of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification, IEEE, New York, NY, USA, IEEE Standard 802.11-1999, 1999

[12] C.K. Toh, "MARCH: a medium access control protocol for multihop wireless ad hoc networks," MILCOM 2000, 21st Century Military Communications Conference Proceedings, 2000

[13] Shugong Xu, Tarek Saadawi, ―Does the IEEE 802.11 Mac protocol work well in multihop wireless adhoc networks, City university of New York, June 2001.

[14] Eustathia Ziouva, Theodore, CSMA/CA performance underhigh traffic conditions: throughput and delay analysis,‖ Journal on computer communications,vol. 25, pp. 313-32, 2002.

[15] Yihong Zhou, Scott M. Nettles, ―Balancing the hidden and exposed node problems with power control in CSMA/CA based wireless networks,‖ IEEE Conference on Wireless Communications and networking, Austin USA, vol. 2, pp. 683-688, 2005.