Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A Realistic study of Mobile Ad Hoc Networks

R. Kalaiarasi[1*] and D. Sridharan[2]
[1]*School of Computer Science, Tamil Nadu Open University, Chennai-600015*
[2]*Department of Electronics and Communication Engineering, CEG campus, Anna University, Chennai-600025*

Abstract — A wireless technology has opened the doors for new emerging applications of networking and one of the emerging and potential areas is the domain of Mobile Ad Hoc Networks (MANETs). MANET is a collection of wireless mobile nodes without the need for centralized access points. In order to achieve better security for the network, secure routing has been used to protect the routing protocol against malicious attaches in MANET. In this article, a detailed study of IEEE 802.11 access mechanism and its vulnerabilities are given.

Keywords—MANET, IEEE 802.11 MAC protocol, Access Method, RTS-CTS Mechanism, Misbehaving Techniques;

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a network of mobile devices that communicates through wireless links without the use of any fixed infrastructure or centralized control [1]. The most distinctive feature of MANET is the lack of any fixed infrastructure compared with the cellular or satellite networks. Mobile devices in ad hoc networks communicate with each other through a multi-hop route, using cooperating intermediary nodes. Each node acts as a router and takes part in multihop communication as shown in Figure 1.

Each node should forward the packets to its neighbours to communicate with far away nodes. Any node can join in the network or can leave the network without any constraint. So, MANET does not depend on a particular node as in an infrastructure network and is very flexible and robust. This type of network has received considerable interest in recent years due to its capability to be deployed quickly without any fixed infrastructure [2]. However, they are subjected to more challenges than the wired networks. These networks face various problems like unpredictable topology, increased interference, congestion and limitation of resources like bandwidth and energy due to shared wireless medium and its dynamic nature.

In MANET, nodes are usually power constrained because they depend on limited battery resources. Wireless communications consume lot of energy for forwarding packets and also for overhearing packets from other nodes. Energy is the main source required to operate the MANET, where some nodes may not forward packets to its neighbors to save their battery power. These types of nodes are called selfish nodes. Selfish nodes try to improve their own performance like throughput, latency etc [3].

@IJMTER-2015, All rights Reserved

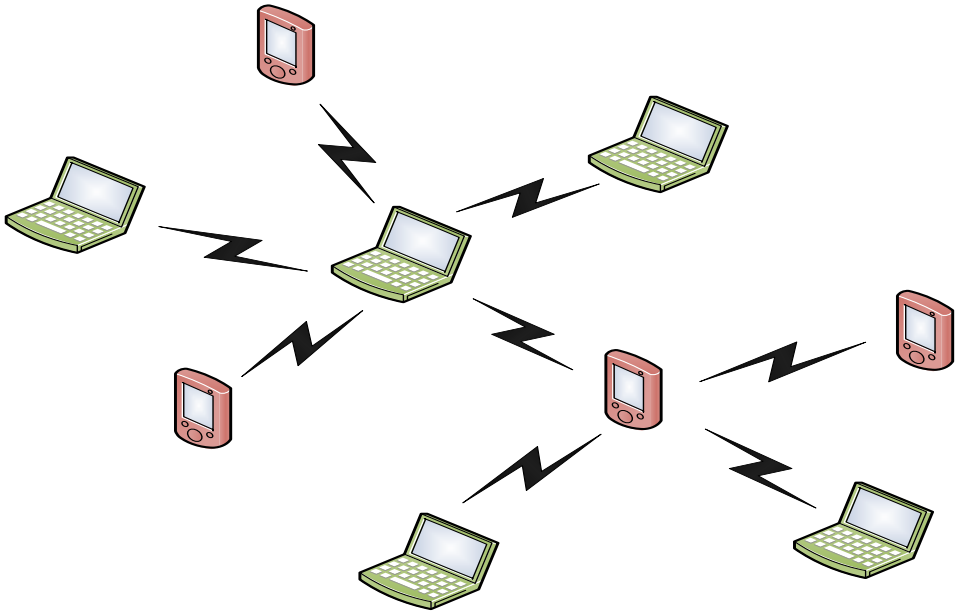

Figure 1. Mobile Ad hoc Networks

II. MANET NETWORK MODEL

Networks are divided into two types based on the topology of the network one is infrastructure network and other is infrastructureless network or Ad hoc Network [4].

2.1. Infrastructure Network

In this type, wireless nodes are connected with the nearest Access Point (AP) that is within its communication radius.

2.2. Infrastructureless Network

A group of mobile nodes are connected with the radio links without any centralized control or AP. It is also known as peer-to-peer network.

III. BACKGROUND OF IEEE 802.11 MAC PROTOCOL

Wireless networks have experienced unparalleled development in the past decade. IEEE 802.11 MAC uses two types of coordination function to access the wireless networks. Firstly, Distributed Coordination Function (DCF), which allows contention access for wireless channel and secondly, Point Coordination Function (PCF), which requires centralized APs. The architecture of the IEEE 802.11 MAC is shown in Figure 2

The contention resolution mechanism is typically based on cooperative protocols (e.g., random backoff before transmission) that attempt to ensure a reasonably fair throughput share for all the participating hosts. In environments where hosts in the network are untrusted, some hosts may misbehave by failing to adhere to the network protocols, with the intent to obtain an unfair share of the channel. PCF is the upper sublayer and DCF is the lower sublayer in the MAC protocol. PCF is a contention free access protocol, which is controlled by centralized point coordinator to support real time traffic. The main drawback of PCF is that it will not work for MANET due to the central coordinator and also it is not commonly supported in commercial products.

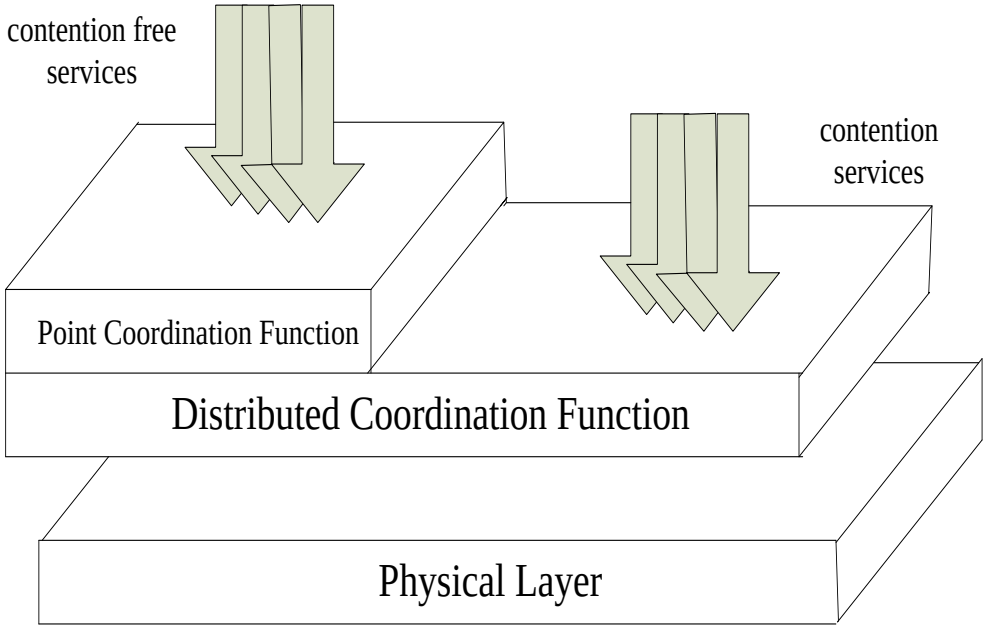

Figure 2. IEEE 802.11 MAC Architecture

DCF is a random access method, which uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to access and reduce the packet collisions. In CSMA/CA networks, a radio station which finds that the radio environment is available will start to transmit only after random backoff procedure [5]. Any node which wishes to transmit will first sense the channel to know the status of the medium (busy/idle). If the medium is busy, the node defers its transmission until the medium is determined to be idle for a duration which is equal to DIFS. If the node is idle for DIFS time, it then enters into the backoff window or contention window.

Backoff time is a random value which can be chosen uniformly from the range 0 to CWmin-1, where CWmin is the minimum contention window size with a standard value of 32 and the maximum contention window size is set to 1024. When the channel is sensed idle, the backoff timer is decremented for every time slot and freezes when the medium is sensed busy. When the backoff timer reaches 0, the node starts its next transmission. The node doubles the contention window for each unsuccessful transmission until it reaches the maximum value CWmax = 2mCWmin, where m is the maximum backoff stage with a standard value of 5. This is known as Binary Exponential Backoff (BEB) algorithm. This will reset to minimum contention window after each successful transmissions [6]. The backoff value is expressed by the following equation

Backoff Counter = INT (Rnd ().CWmin)

Where, Rnd () is a function that returns pseudorandom numbers uniformly distributed in (0, 1) [7].

DCF defines two types of carrier sensing mechanism. First one is called physical carrier sense, which is supported by the physical layer. Second one is virtual carrier sense, which is supported by the MAC layer.

3.1 Basic Access Method

DCF includes both basic access method and an optional channel access method using Request To Send / Clear To Send (RTS/CTS) exchanges. Basic access mechanism is a two way handshaking method where only data and ACK are exchanged which is shown in Figure 3 When the transmitter transmits data to the receiver after Short Inter-Frame Space (SIFS) interval, the receiver replies with

the ACK control frame. If ACK is not received by the sender within the specified ACK_Timeout period then, the frame is assumed to be lost and schedules the retransmission.

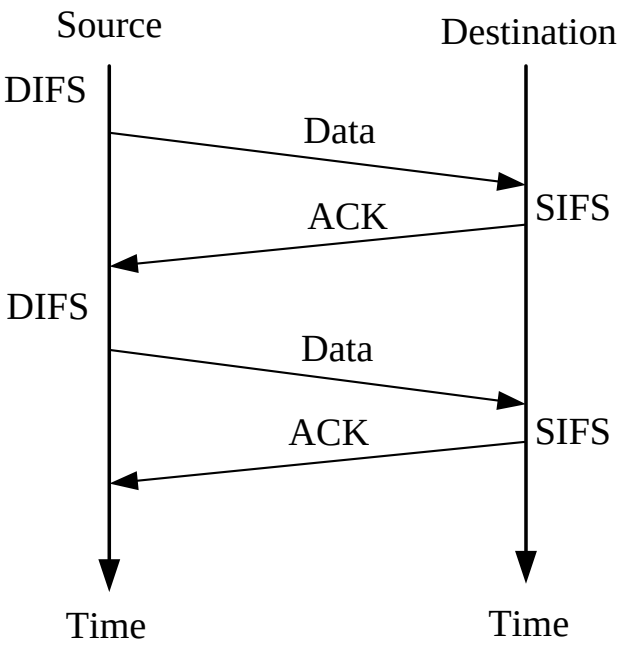

Figure 3. IEEE 802.11 basic access handshake

3.2. RTS-CTS Mechanism

In RTS/CTS access method, when the node needs to transmit a data frame it should wait until the channel is sensed idle for DIFS time and backoff time. Then only the node can transmit short RTS control frame instead of data frame. After a SIFS interval the receiver replies with the short CTS control frame. This RTS/CTS exchange ensures that both the sender and receiver are ready to transmit and receive the frames which are shown in Figure 4.

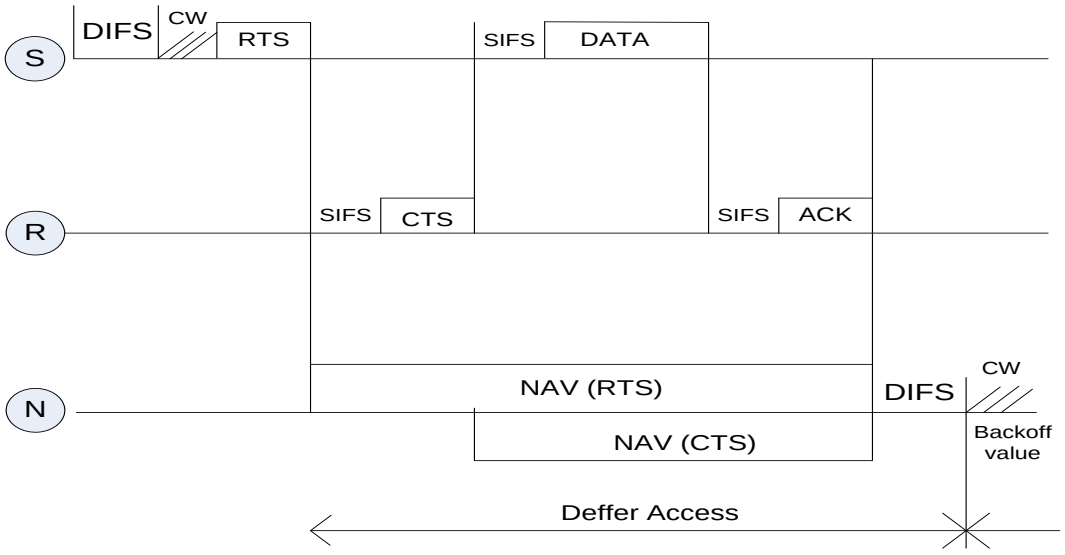

Figure 4. IEEE 802.11 RTS/CTS Mechanism

Both the RTS and CTS frames contain details about the length of the frame to be transmitted. Neighbouring nodes which overhear the RTS and CTS control packets will update their Network Allocation Vector (NAV). NAV is a timer which is included in the duration field of RTS, CTS control frames. When the NAV timer becomes 0, neighbouring nodes can start their transmission, otherwise it would be silent. Now the sender sends data packets after the SIFS interval. The receiver replies with ACK to confirm the reception of the data packets. SIFS period is shorter than the DIFS period, which guarantees continuous RTS+CTS+DATA+ACK exchange [8].

IV. MISBEHAVING TECHNIQUES

In the Data link layer, in order to achieve an operational point in the network, all the CSMA/CA schemes assume that all participants should strictly follow the protocol specifications. However, especially in the presence of autonomous nodes this assumption may not always be valid. Unfortunately, there are various ways in which a station can gain advantage [9] by not adhering to the protocol guidelines like:

- Choosing small backoff values: A selfish node can choose a smaller value instead of choosing randomly.
- Not doubling CW after collision: A node may not invoke the collision recovery procedure after collision. Thus, the node would always be choosing its backoff values from [0, CWmin], thereby utilizing values for backoff.
- Manipulating the NAV value: If a node increases this value, it can assure that all other agents will remain idle even after the end of current transmission.
- Not confirming to the DIFS and SIFS intervals: This behavior will increase the chances of getting access to the medium.
- Magnify the value of the duration field in RTS or DATA packets such that the receivers keep silence for a period larger than the real transmission time. As a result, if the cheater node has more packets to send, it gets more chance to access the medium, as it starts counting down its backoff before its neighbors.
- When the channel is sensed to be idle, it transmits before the required DIFS time slots elapses, i.e. the misbehaving node waits for a shorter period called S-DIFS (Short-DIFS).

V. CONCLUSION

Mobile ad hoc network is the emerging technology in the recent years. An attempt has been made to analyse the security threats relating to adhoc networks. Here, a detailed study of IEEE 802.11 access mechanism and its vulnerabilities are presented.

REFERENCES

[1] Perkins, CE, Royer, EM & Das, SR, 'Performance evolution of two on-demand routing protocols for ad hoc networks,' Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 2001, vol. 1, pp. 3-12.

[2] Priyanka Goyal , Sahil Batra , Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks , International Journal of Computer Applications, 2010, Vol. 9, No.12, pp 975-987.

[3] Chunfeng, L, Yantai, S, Mingyuan, L & Yang, 'A new mechanism to detect selfish behavior', IEEE 802.11 Ad Hoc Networks, Proceedings of the IEEE international conference on communications, 2009, pp.4918-4922.

@IJMTER-2015, All rights Reserved

[4] Kyasanur, P & Vaidya NH, 'Detection and handling of MAC layer misbehavior in wireless networks', Proceedings of the international conference on dependable systems and networks, 2003, pp.173-182.

[5] Potorac, AD 'Considerations on VoIP throughput in 802.11 networks' Advances in Electrical and Computer Engineering, 2009, vol. 9, no. 3, pp. 45-50.

[6] Tang, J, Cheng, Y & Zhuang, W 'Real-Time Misbehavior Detection in IEEE 802.11 Based Wireless Networks: An Analytical Approach', IEEE Transactions on Mobile Computing, IEEE computer Society Digital Library, IEEE Computer Society, 2012, vol. 11, no. 10, pp. 1624-1632.

[7] Cagalj, M, Ganeriwal, S, Aad, I & Hubaux, JP 'On Cheating in CSMA/CA Ad Hoc Networks', Technical Report IC/2004/27, EPFL-DI-ICA, 2004,

[8] Konorski, J 'A Game-theoretic study of csma/ca under a backoff attack', IEEE Transactions on Networking, 2006, vol. 14, no. 6, pp. 1167- 1178.

[9] PP Kotzias, ''Security Attacks and IDS solutions in Mobile Ad Hoc Networks" Thesis, University of Piraeus December 2011, pp.1-57

@IJMTER-2015, All rights Reserved