International Journal of Engineering Research (ISSN : 2319-6890)
Volume No.1, Issue No.1, pp : 04-08 01 Nov. 2012

Comparison of Performances of MAC Protocols of Wireless Networks under Misbehaving Condition

Neha Singh Sisodiya, Sarita Singh Bhadauria
Department of Electronics & Communication, M.I.T.S., Gwalior, M.P., India
nehasinghsisodiya@gmail.com , saritamits61@yahoo.co.in

Abstract- In this paper the performances of two major mac layer protocols i.e. 802.11 and CSMA/CA is compared when the number of selfish nodes increases in the wireless networks. Selfish nodes try to acquire more bandwidth and large throughput in compare to legitimate nodes. In this way it will be easy to find that 802.11 is better to use than CSMA/CA MAC protocol. The performances of both protocols determined by the qualnet-5.2 simulator which is very user friendly and appropriate.

.***Keywords -*** Distributed Coordination Function, 802.11 MAC Protocol, Selfish misbehavior, CSMA/CA

1.INTRODUCTION

Communication protocols were designed under the assumption that all nodes would obey the given specifications. However when these protocols are implemented in an untrusted atmosphere , a misbehaving node can deviate from the protocol specification and achieve better performance at the expense of honest participants . In this paper we focus our attention to misbehavior at the IEEE 802.11 MAC layer protocol and of CSMA/CA protocol. Examples of misbehavior at the MAC layer can include modifying the parameters for accessing the channel in order to obtain a better throughput, or a network card with an inaccurate implementation of parameters.

A user modifying the parameters to access the channel to obtain a better throughput said as misbehaving at the MAC layer in wireless. These misbehaving nodes are able to utilize most of the available network resources, degrading other well behaving users performance by misbehaving. The IEEE 802.11 distributed coordination function (DCF) method purpose is carrier sensing with collision avoidance and is designed as one of the most popular MAC layer access protocols for wireless networks including CSMA/CA.

The IEEE 802.11 protocol designed with the assumption that all nodes are fully cooperative and follow the rule[2]. However, some nodes choose to deviate and show misbehavior at the MAC layer. These type of misbehaviors at MAC layer highly effect the performance of the network in terms of overall throughput and fairness. IEEE 802.11 MAC protocol consist of two mechanisms generally one for contention resolution centralized mechanism called Point Coordination Function (PCF) and a fully distributed mechanism called Distributed Coordination Function (DCF).PCF needs a centralized controller (such as a base station) which controls all nodes activities and used in infrastructure-based wireless networks. DCF is used in both infrastructure-based wireless networks as well as ad hoc wireless networks.

In this paper, we compare misbehavior possible in the DCF mode of wireless network. DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA), and solves the hidden terminal problem based on its optional request-to-send (RTS) and clear-to-send (CTS) . The fundamental access method of the IEEE 802.11 MAC Protocol is a DCF known as Carrier Sense Multiple Access with collision avoidance (CSMA/CA) [12]. The CSMA/CA contains of the basic access mode as well as the optional RTS/CTS/ACK access mode. In basic access mode, a node senses the channel to find whether another station is transmitting before initiating a transmission. If the medium is sensed to be free for a DIFS interval time, the node transmits. If the medium is busy, the node defers its transmission until the end of the current transmission. Then, it will wait for an additional DIFS interval time and generate a random backoff time to initialize the backoff timer before transmission. The backoff timer is decreased as long as the medium is idle and suspended when a transmission is detected on the channel, and resumed when the medium is sensed as idle again for more than a DIFS interval. Only when the backoff timer reaches to zero, the node transmits its packet. The destination node waits for SIFS duration and transmits ACK packet.

In RTS/CTS access mode , after obtaining the channel access right, the sender sends an RTS frame before data transmission to announce the upcoming transmission. When the destination node receives the RTS frame from sender, it will transmit a CTS frame after a SIFS interval. Both the RTS and CTS frames are short control frames. The source node is allowed to transmit its packets only if it receives the CTS frame correctly from receiver.

The remaining paper is organized in the following way. II part gives overview of the related work. The III part gives an idea about the MAC protocol that how it works. The IV-A part explains the misbehavior detecting method. IV-Bsection describe the technique for assigning backoff so that the overall performance of the network can be improved. Section-V reports the simulation and discuss the results. Section VI concludes the paper.

2. RELATED WORK

In [9] authors proposed a MAC selfishness hindering detection process and correction mechanism. Their main idea was to allow the reciever to distribute and send back value in the CTS and ACK frames, and then to use the values to detect the misbehaviors. The correction program is that if selfish behavior is detected, punishment will be executed at the next backoff time. Cagalj in [10] used a game-theoretic frame to study the selfish behavior of MAC layer. Through a dynamic game model, he got a more balanced strategy for the network. In this model, each node controls its own channel access probability by adjusting its own contention window size. This model is effective when all nodes are within the scope of their respective network.

The authors of [4] discuss the same problem and proposed a system, DOMINO, to detect greedy misbehavior and backoff manipulations of IEEE 802.11. Alternatively, malicious misbehavior aims primarily at disturbing the normal operation of the network [6]. This includes colluding adversaries that continuously send data to each other in order to deplete the channel capacity (i.e., causing a denial of service attack, DoS) and hence prevent other legitimate users from communicating [8].

The authors in [5], [7] address the detection of an adaptive intelligent attacker by casting the problem of misbehavior within the minimax robust detection framework. They optimize the s performance of the system for the worst-case instance of uncertainty by identifying the least favorable operating point of a system and derive the strategy that optimizes the system's performance when operating at that point. System performance is measured in terms of number of observation samples required to derive a decision (detection delay).

Since nodes that form an ad hoc wireless network are expected to move freely, there has been a multitude of mobility models [14] introduced. These models control either the movement of individual nodes or the movement of groups of nodes. A well-known mobility model is the *Random way point model*. In this model, nodes move from the current position to a new randomly generated position at a predetermined speed. After reaching the new destination a new random position is computed. Nodes pause at the current position for a period t before moving to the new random position. Other mobility models, commonly used, are: Random walk model, Random direction model, Gaussian-Markov model or Nomadic community model .

3. MAC PROTOCOL DESCRIPTION

In wireless networks, distributed MAC is preferred, because the network itself is distributed in essence. Whenever a centralized MAC is used for these networks, it lacks enough efficiency owing to the need for maintaining the centralized control among various nodes. PCF also inhibits the scalability of the MAC protocol. As a result, distributed MAC is necessary for MANETs, and also for Wireless Networks. However, it is sure that designing a distributed MAC is a much more challenging task than configuring a centralized MAC.

A. IEEE 802.11s MAC Overview

The 802.11 protocol specifies a common medium access control (MAC) layer, which includes a variety of functions that support the operation of wireless LANs. Generally, the MAC layer manages as well as maintains communication between 802.11 stations (radio network cards and access points) by cooperating access to a shared radio channel and using protocols that enhance communication of a wireless medium. Inspite of viewing as the "brain" of the network, the 802.11 MAC layer uses a physical layer, such as 802.11b or 802.11a, to perform the work of carrier sensing, transmission, and reception of 802.11 frames. The IEEE 802.11 MAC protocol consist of two types of access methods.

The basic access method used is the distributed coordination function (DCF), which is a carrier sense multiple access with collision avoidance (CSMA/CA) mechanism. It was created to support best effort traffic, like internet data. Moreover, IEEE 802.11 also incorporates an optional access method in which access point do the polling to determine which station has the data to transmit resulting in a contention free communication. This method is known as the point coordination function (PCF) and is mostly used in scenarios where service guarantees are needed. It was stated previously, PCF is an optional access mechanism which can be used only in the presence of an access point; concurrently with DCF. Since the concentration in this paper is on the Wireless Networks, therefore DCF will be the primary access method. A brief description of DCF in context of this study is as follows.

B. Selfish MAC layer Misbehavior

The nodes which misbehave can be classified into two types. First kind of called selfish nodes, and the second are called malicious nodes. A selfish node is only interested in about improving its performance even at the expenses of other nodes. The malicious nodes intends to disrupt normal network operations, like denial of service (DoS) attacks, or jamming the wireless channel to prevent communication, etc.

In order to prioritize access to the wireless medium, DCF defines three time windows (SIFS, DIFS, and EIFS), only the first two are important for the purpose of our discussions. Prior to the transmission of any frame, a node must observe a quiet medium for one of the defined window periods. The short interframe space (SIFS) is used for the frames sent as part of preexisting frame exchange (e.g., CTS or ACK frames sent in response to previously transmitted RTS or DATA frames). DCF Interframe Space (DIFS) is used for nodes wishes to initiate a new frame exchange. After the channel is sensed idle for a DIFS time by node, a node waits for an additional backoff time after which the frame is transmitted.

To completely manipulate the channel, a node could transmit a signal after a short SIFS and to achieve a notable increase in the bandwidth a node could transmit after SIFS but before DIFS when the channel is idle . However, as shown in, there are other consequences resulting from selecting different values of SIFS. Whenever a node has a packet to transmit it will sense the medium for a duration of DIFS. If the channel is sensed busy, the sender defers its transmission by starting its backoff algorithm. If the medium is idle for a DIFS period, it then performs an RTS/CTS exchange before the actual data transmission to reserve the shared medium to reduce the high probability of collision. After a successful transmission of DATA, the receiver sends ACK back to the sender.

C. CSMA PROTOCOL DESCRIPTION

In CSMA-based schemes, the transmitting node first senses the medium and check whether it is idle or busy. The node defers its own transmission to prevent a collision with the existing signal on the network, if the medium is busy. Otherwise, the node begins to transmit its data while continuing to sensing the medium. However, collisions occur at receiving nodes. Since, signal strength in wireless medium fades in proportion to the square of distance from the transmitter, the presence of a signal at the receiver node may not be clearly detected at other sending terminals, if they are out of range. As shown in Fig. 1, node *B* is within the range of nodes *A* and *C*, but *A* and *C* are not in each other's range. Let us consider the case where *A* is transmitting to *B*. Node *C*, being out of *A*'s range, cannot detect carrier and may therefore send data to *B station*, thus causing a collision at *B*. This is referred as the '*hidden-terminal problem*', as nodes *A* and *C* are hidden from each other. Let us now consider second case where *B* is transmitting to *A*. Since *C* is in *B*'s range, it senses carrier and it decides to defer its own transmission. However, it is not necessary because there is no way *C*'s transmission can cause any collision at receiver *A*. This is referred to as the '*exposed-terminal problem*', since *B* being exposed to *C* caused the later to needlessly defer its transmission . MAC methods are designed to overcome these problems.

4. SIMULATION RESULTS

We have taken a network with 20 nodes distributed randomly in a 500m· 500m square area network. The transmission range of each node is 250m. Here 6 cbr connections are made.The mobility mode used is random way point model. The simulation time is 500 seconds. The routing protocol is AODV. The power save mode is also enable here. Size of CBR packet is taken 512 bytes.We compared the impact of this attack on 802.11 and CSMA Mac Protocols using three parameters: end-to-enddelay,throughput and jitter. We carried out the simulation experiments scenarios changing the following parameters: percentage of attacker nodes, random way point mobility is chosen. Each result is the average value of 10 simulation runs often used. And the comparison of unicast packet sent and unicast packet received is shown as well as the comparison of the broadcast packet sent and broadcast packet received is also shown in figures

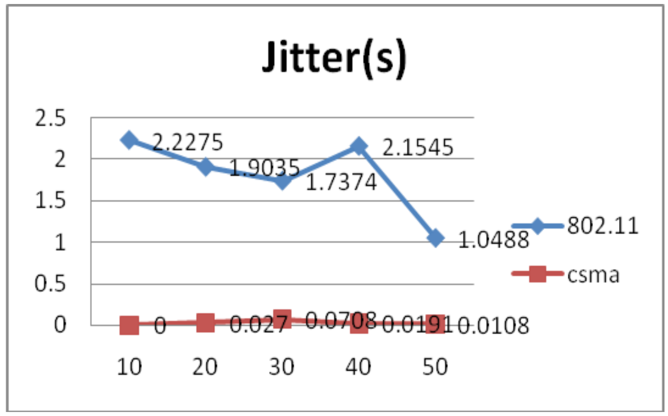

Fig 1 Percentage of attackers

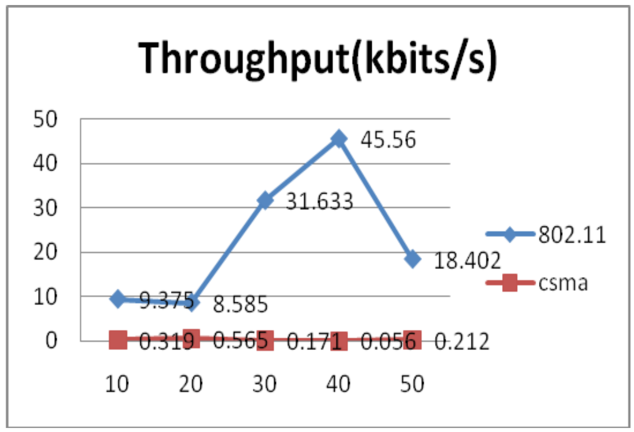

Fig 2 Percentage of attackers

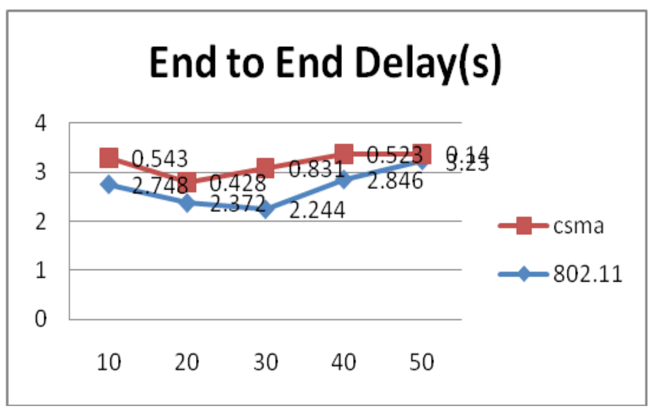

Fig 3.Percentage of attackers

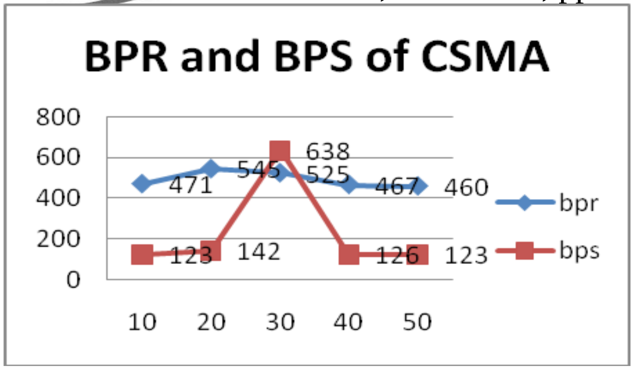

Fig 4 Percentage of attackers

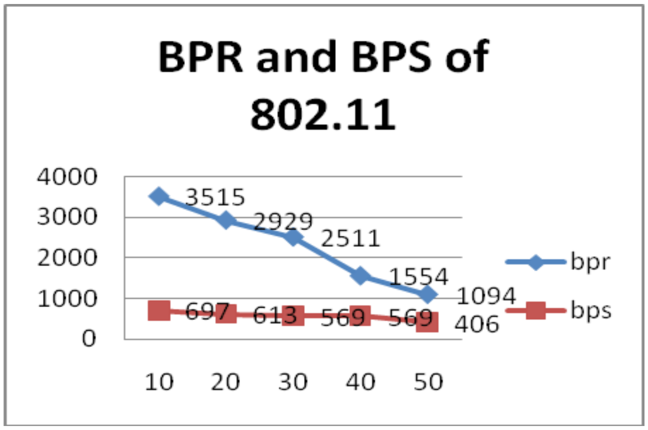

Fig 5 Percentage of attackers

Here it can be seen clearly that performance of 802.11 is better than CSMA protocol in a misbehaving atmosphere. Also the difference between the BPR and BPS is more in case of CSMA than 802.11 Mac Protocol.

Here qualnet 5.2 is used for the network simulation and it is very user friendly.

5.CONCLUSION AND FUTURE WORK

In this paper the performance of 802.11 mac protocol is compared with CSMA in the presence of misbehaving nodes .Several parameters which are important including throughput and jitter are shown. It is clear here that the efficiency of a network using CSMA get down in the presence of selfish nodes than 802.11.

For future work both protocols can be compared in different scenario like varying pause time and other parameters also.

REFERENCES

[1.]Vamshikrishna Raseddy Giri Neeraj Jaggi “MAC Layer Misbehavior Effectiveness and Collective Aggressive Reaction Approach.”

[2]. Sam Jabbehdari, Anahita Sanandaji, and Nasser Modiri “Evaluating and Mitigating the Effects of Selfish MAC Layer Misbehavior in MANETs.” JOURNAL OF COMPUTING, VOLUME 4, ISSUE 2, FEBRUARY 2012, ISSN 2151-9617

[3]. Pradeep Kyasanur, Nitin H. Vaidya “Detection and Handling of MAC Layer Misbehavior in Wireless Networks” Proceedings of the 2003 International Conference on Dependable Systems and Networks (DSN’03) 0-7695-1959-8/03 $17.00 (c) 2003 IEEE

[4]. M. Raya, J.P. Hubaux, and I. Aad, “DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots,” *IEEE Transactions on Mobile Computing*, 5(12), 1691–1705, 2006

[5] S. Radosavac, J. S. Baras, and I. Koutsopoulos, “A framework for MAC protocol misbehavior detection in wireless networks,” in *Proceedings of the 4th ACM workshop on Wireless Security (WiSe 05)*, 2005, pp. 33–42

[6] L. Guang and C. Assi.Vulnerabilities of ad hoc network routing protocols to MAC misbehavior.In *IEEE/ACM WiMob*, August 2005.

[7] S. Radosavac, G. V. Moustakides, J. S. Baras, and I.Koutsopoulos, “An analytic framework for modeling and detecting access layer misbehavior in wireless networks,” *submitted to ACM Transactions on Informationand System*

[8]Y. Zhou, D. Wu, and S. Nettles. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems. In *Workshop on BWSA, BROADNETS*, October 2004.

[9] P. Kyasanur and N. Vaidya, “Selfish MAC Layer Misbehavior in Wireless Networks,” IEEE Transactions on Mobile Computing, vol. 4(5), 2005, pp.502–516.

[10] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P.Hubaux, “On selfish behavior in CSMA/CA networks,” Proc. IEEE INFOCOM, vol. 4, 2005, pp. 2513–2524.

[11] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks .*Mobile Computing*, 353:153–181, 1996.502, 2002.

[12] ANSI/IEEE Std 802.11, 1999 Edition. http://path.berkeley.edu/dsrc/reading/st3.pdf