Mitigating Misbehaving Node Using Receiver Network Allocation Vector

R. Kalaiarasi and D. Sridharan

Abstract—In MANET, MAC layer uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism to access the medium. This mechanism allows contention to access the medium among the competing nodes. Misbehaving nodes may violate the IEEE 802.11 MAC protocol rules to increase their throughput at the expense of other nodes. In order to rectify this drawback, the misbehavior nodes have to be detected to improve the network performance. Hence, the proposed work involves the detection of misbehaving node using the contention window value. In addition, The RNAV (Receiver Network Allocation vector) timer is to be fixed at the receiver side to avoid the collisions.

Index Terms—IEEE 802.11 protocol, manet, misbehavior detection, RNAV.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) [1] has recently been the topic of extensive research. In recent years, Mobile Ad-hoc networks (MANET) became very popular because of its instant infrastructure where the wireless networks are not available. In MANET each node can communicate via wireless links if it is within the radio transmission range. Some nodes are away from the transmission range. Due to the out of transmission range, nodes cannot communicate directly. Source node can relay messages between the intermediate nodes to ensure communication at the destination. MANETs can be used in military applications, emergency situations like earthquakes, fire and conferences.

Ad hoc networks inherits most of the traditional wireless network problems, such as interference, low reliability, low bandwidth, high influence of the environment for the correct functionality of the network, limited resources in terms of battery and processor power and low service coverage [2]. IEEE 802.11 Medium Access Control (MAC) protocol uses a contention resolution mechanism for sharing the wireless medium. Due to the open wireless medium, MANET should cooperate to forward the messages if it is outside the transmission range. Increased programmability of network devices lately [3] has led to the possibility of individual users modifying their own protocol parameters in order to achieve higher bandwidth. Such misbehaviors at the MAC layer adversely affect the performance of the network in terms of overall throughput and fairness and are quite intense when distributed coordination function (DCF) mode of 802.11 operations in used [4].

The remainder of this paper is organized as follows: section II deals with the IEEE 802.11 DCF protocol, in section III presents the overview of the related work, section IV describes the proposed architecture, section V gives the simulation analysis and section VI concludes the paper.

II. IEEE 802.11

The IEEE 802.11 standard [5] specifies two types of coordination functions for stations to access the wireless medium. Distributed Coordination Function (DCF) and Point Coordination Function. DCF is a contention based protocol which uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to access the channel. In this technique several users attempt to access the common shared channel in a random manner. A node wishing to transmit data, first senses the medium using virtual carrier sensing mechanism. Virtual carrier sensing [6] considers the medium as idle if Network Allocation Vector (NAV) is zero, otherwise it considers the medium busy.

Request to send/Clear to send (RTS/CTS) control packets includes the transmission time of all the packets in the sequence. If the channel is sensed idle for DIFS time, then the sender immediately starts transmitting the data. Otherwise, the station waits for DIFS time and then waits for a random back off interval which is uniformly chosen between [0, CWmin], where CWmin is the minimum contention window[7]. During the above said period the medium is busy, so it waits for NAV count to become zero. After the back-off counter (NAV) counts down to zero it start transmitting data to the receiver.

The receiver successfully receives the data packet, sends ACK after waiting for a SIFS time. If the transmitter does not receive ACK frame, it doubles the contention window size. Otherwise it resets the contention window to CWmin. A selfish node can deplete the channel capacity within its vicinity in a congested environment by manipulating the back off procedure of IEEE 802.11 (CSMA/CA) [5]. Misbehaving nodes may choose small back-off values to gain more access from the network. So misbehaving nodes continuously selecting small contention window to get more throughput than other contending nodes.

![Fig. 1. Structure of RTS/CTS mechanism](image)

Manuscript received October 20, 2012; revised November 25, 2012.
R. Kalaiarasi and D. Sridharan are with Dept. of Electronics & Communication Engineering, Anna University, Chennai, India (e-mail: kalaiarasidr @ gmail.com; Sridhar @ annauniv.edu).

DOI: 10.7763/IJCEE.2013.V5.667

76
The receiver successfully receives the data packet, sends ACK after waiting for a SIFS time. If the transmitter does not receive ACK frame, it doubles the contention window size. Otherwise it resets the contention window to CWmin. A selfish node can deplete the channel capacity within its vicinity in a congested environment by manipulating the backoff procedure of IEEE 802.11 (CSMA/CA) [5]. Misbehaving nodes may choose small back-off values to gain more access from the network. So misbehaving nodes continuously selecting small contention window to get more throughput than other contending nodes. After a successful transmission according to IEEE 802.11, a node would select a back-off value randomly from 0 up to CW-1. By selecting a small contention window, the selfish node waits only for a short period of time for accessing the medium. Due to this, well behaved nodes lose their regular accessing chance to the misbehaved nodes. This will degrade the performance of network operation.

### III. RELATED WORK

Several detection and reaction schemes have been proposed to detect the MAC layer misbehaviour. The authors of [8] have presented a detection system called DOMINO, which does not require any modifications in the MAC protocol standard. This system is implemented at the AP and assumed to be more reliable. In the first phase, traffic traces of sending hosts are collected periodically during short intervals of time. At the second phase, the collected data then passed to the DOMINO algorithm to detect the deviation node. Outputs of the algorithm send it to the decision component to check whether the given node is misbehaved or not. But it fails to detect the adaptive cheater.

Carrier Sensing based Discarding (CSD) scheme [9] has several carrier sensing points. These are randomly set among the entire data packet transmission to detect the misbehaving node. CSD needs many detection points to verify the ongoing data communication.

In [2] authors have proposed Predictable Random Backoff (PRB) algorithm to mitigate selfish MAC layer misbehaviour, which is based on the modifications of Binary Exponential Backoff (BEB) algorithm.

### IV. PROPOSED ARCHITECTURE

#### A. Identifying Deviation from the protocol

The proposed scheme is designed to handle selfish MAC layer misbehavior in IEEE 802.11 hotspots. The sender sends a RTS frame after waiting for backoff time selected from the range [0-CW]. It can select any value within the above range. This approach uses contention window value that enables the receiver to identify the sender misbehavior within a small observation interval. The backoff of a sender is counted as the idle period from the successful transmission of a previous frame to the next transmission from the same sender. This approach uses idle duration, Distributed Inter Frame Space (DIFS) value and time duration of each slot. Using the above said value receiver calculates the CW selected for current transmission. This is the Actual Contention Window value calculated by the receiver. From the equation (1) Actual contention window selected for current transmission can be calculated [10].

$$T_{bo}=T_{DIFS}+CW*T_{slot}$$  \(1\)

where Tbo is the idle duration, TDIFS is the value of Distributed Inter Frame Space (DIFS) and Tslot is the time duration of each slot.

If the node is a selfish node it keeps on selecting the small CW. Receiver sets the Threshold for every RTS transmission. Receiver increases the Threshold value till it reaches the maximum threshold limit. Receiver observes the CW selected for every transmission and calculates the average observed value and compares the actual contention window with the observed backoff value. If the observed value is less than the Actual backoff value the sender node deviates from the MAC protocol rules causing violation.

In the presence of collisions, the receiver will find it difficult to judge whether a node increases its contention or not [10]. Therefore the RNAV (Receiver Network Allocation Vector) is set at the receiver side [11] in the duration field of RTS frame. RNAV timer has the transmission time of RNAV after receiving RTS message. Any node entering into the network will check the RNAV value to communicate with the receiver. If RNAV is greater than zero it waits till the value reaches zero.

Once the RNAV becomes equal to zero the receiver can communicate with any other node. Using RNAV value, collision can be avoided at the receiver side.

#### B. Penalty Calculation

Misbehaving node may deviate from the protocol by obtaining a larger throughput share than well behaved nodes. After detecting a host deviating from the protocol, measure the difference between the Actual contention value and observed value. Well behaved nodes penalizes by assigning large backoff value to the misbehaving nodes. To prevent misbehaved node, add the penalty time to access the medium.
Adding penalty time is to discourage the misbehaving node [6].

\[
\text{New backoff} = \text{old backoff} + \text{penalty} \quad (2)
\]

Penalty is the measured deviation from the maximum of acw-observed value. Receiver node calculates the new backoff value to punish the sender. The deviating sender assigns random value plus penalty for the next backoff.

RNAV Algorithm

Initially calculate the contention window using

\[
T_{\text{cw}} = DIFS + \text{CW} \times T_{\text{slot}}
\]

Set RNAV at the receiver side

If RNAV > 0

\(\text{Receiver is busy, no transmission}\)

If RNAV = 0

\(\text{Neighbouring nodes can transmit}\)

If acw > average observed value

\(\text{Status = misbehavior}\)

V. SIMULATION ANALYSIS

Simulation Analysis is being implemented in Network Simulator (NS-2) with the following assumptions. The simulation scenario is created with 30 nodes. Among them, 15 nodes are senders and 15 nodes are receivers. The transmission radius is 250 meters. Simulation area is 500 m². The traffic type from source to destination is Constant Bit Rate (CBR) and packet size is 512 bytes/packet. The data rate is 4 packets/second. Total simulation time is 60 seconds. To identify the possible misbehaving nodes, observing node needs to measure certain aspect in order to analyze the network performance. Throughput is the most important metric to identify the presence of misbehaving node. Packet delay can also be measured to improve the quality of service.

VI. CONCLUSION

We have presented a framework to detect and prevent MAC layer misbehavior. Increasing the user friendly nature of mobile ad hoc networks, it is important to understand the possible misbehaving nodes and safeguard against them. In the proposed work a mechanism has been introduced to detect the MAC layer misbehavior, which is based on calculating the contention window and RNAV timer. By setting RNAV timer at the receiver side, the misbehaving node can be detected. So that the network performance can be improved. The changes in MAC layer standard require exhaustive research and should be tested for the correctness in detail.

REFERENCES