Identifying and Averting the MAC Layer Misbehavior in AD-HOC Networks

Mary Cherian, PhD
Associate professor
Dept. of CSE
Dr. Ambedkar Institute of Technology,
Bangalore, India

Nikita Singh
Dept. of CSE
Dr. Ambedkar Institute of Technology,
Bangalore, India

ABSTRACT

The all-encompassing nature of the ad- hoc network and its design architecture in the multi-hop communication system, where trust value of the participant nodes cannot be necessarily taken for granted, is prone to selfish misbehavior by participant nodes. Therefore, the compliance of the MAC layer protocol has become pertinent to the proper functioning of the network. The optimal performance of the network and the judicious and fare usage of network resources can only be achieved by reliable and timely detection of illegitimate protocol operation. In this paper, it is envisaged that the determination factor quantifies the probability of the misbehavior whereas the trust value quantifies the probability of the well-behaved nodes. Thus, these values provide fair insight into the behavioral pattern of any ad-hoc network. The robust detection framework is, therefore implemented to timely notification of the selfish node. Here, the inherent defense mechanism is also incorporated which enhances efficiency, efficacy of the network and provides fare utilization of resources among the nodes. Proposed scheme is validated through simulation results using NS2.

Keywords

Ad-hoc networks, selfish misbehavior, MAC layer, determination factor, trust value.

1. INTRODUCTION

Mobile ad hoc communication networks are pervasive in nature and due to the wide spread disruptive nature of MANET, it is very difficult to trust the users that, all will comply with the set of protocols. But usually communication protocols are designed under the assumption that all the participants would comply with the regulations. A MANET is a group of independent nodes that form a dynamic, multi-hop radio network in a distributive structure. MANET nodes can be a variety of mobile devices such as mobile phones, laptops, or handheld devices, which present various computation and bandwidth capabilities. The networks can be easily designed, devised and implemented at short notice at various scenarios such as hospitals, battlefields and disaster recovery & rescue operations.

The misbehaving nodes can deviate from the regulation and impair performance of the network and will try to gain unscrupulous advantage over other users. It is imperative in ad-hoc MANET for users to fully adhere to regulations to facilitate the correct route establishment for the successful delivery of the packets and efficient usage of the network resources, thus enhancing network performance optimally. The traditional methods of eliminating the misbehavior based on the cryptography cannot be used to address the misbehavior at Medium Access Layer (MAC).

The MAC layer misbehavior is generally classified into the two categories i.e. malicious misbehavior and selfish misbehavior. Malicious misbehavior is by jamming the network, attacking the network with act of Denial of Service (DoS) [1] and Distributed Denial of Service (DDoS). The malicious user will generate a lot of traffic to overwhelm the network or transmit fake packets to grab the excessive bandwidth on shared channel thus preventing the normal user from communicating. In other type of malicious behavior i.e. in Sybil attack, the large number of fake identities will be forged to disturb the network and genuine users will not be able to access channel.

The wireless network adapters and devices have become easily programmable because of the increased level of sophistication in the design of protocol component. As a result, the tampering of software and firmware by users, have become prevalent and abuse of the network resources have become widespread. The goal of the misbehaving users ranges from exploitation of the network resources to the disruption of the communication itself. The solution to the problem is as follows. First, timely detection of misbehavior instances. Second, isolation of the selfish nodes efficiently with focus on the defense against such instances. However, the difficulties faced are, the randomness of protocols and volatility of the network. Therefore, it becomes extremely difficult to distinguish between genuine attack and protocol malfunction in the wireless network link impairment.

2. LITERATURE SURVEY

There are several works existing in the literature which describe the detection scheme. V. Gupta et al. in [1] analyze the attacks that prevent the user to access channel by causing excessive traffic in ad hoc networks. They mainly focused on the medium access control (MAC) protocol and IEEE 802.11x MAC protocol properties, which activate such attacks. Conventional methods used in wireline networks will not be able to help in prevention or detection of such attacks. It also considered the intelligent attackers those generate traffic patterns which cause denial of service. M. Raya et al. in [2] describe how a greedy user increases its bandwidth at the expense of other users, in particular with the new generation of adapters. They proposed a software called DOMINO [2] that is installed in the Access Point that can easily detect greedy stations. It does not modify the protocol installed at the Access Point. In [3], the authors provide a detection rule for optimum performance worst-case attack. Their aim is to provide a solution with the help of mini max robust detection framework. This basic model is used for studying misbehavior because it deals with the presence of uncertainty of attacks and concentrates on the attack which causes performance loss.

Earlier works residing in the defense schemes are as follows. J. Konorski [4] designs a noncooperative game for wireless LANS which obtains a fair distribution of bandwidth via two policies namely RT/ECD and RT/ECD-1s. Pradeep Kyasanur and Nitin H. Vaidya [5] proposed a scheme in which receiver interprets that a sender can access a channel without waiting for an assigned back off which detects selfish misbehavior. In this situation, a penalty is added by the receiver to the sender's next assigned back off. The probability of detecting selfish misbehavior increases when sender is unable to back off for a time interval specified by the penalty.

3. DETAILED DESCRIPTION OF THE PROTOCOL

The detailed description of the protocol is provided in this section

3.1 IEEE 802.11 DCF (Distributed Coordination Function) [6]

IEEE 802.11 DCF implements CSMA\CA scheme for medium access protocol (MAC). MAC layer protocol determines the methodology to access channel. When a node wants to send a data to the destination, it senses the channel, if the channel is busy it waits for DCF Inter Frame Space (DIFS) duration and after expiry of DIFS duration, will again start sensing a channel. If a channel is idle, it waits for a back off time period. During back off time, if channel again becomes busy, the back off time gets suspended and same the procedure is repeated again. After the back off time reduces to the 0, the node starts transmitting data via four way handshake. According to the four way handshake procedure, sender first sends a RTS to the receiver. On successful receipt of the RTS, the receiver responds with a CTS. After listening to the RTS, other neighboring nodes update their Network Allocation Vector (NAV) and will sense the channel again when NAV expires. On successfully receiving CTS, sender starts sending the data. The transmission stops until the receiver successfully sends an acknowledgement. During the first transmission, the sender keeps its window size minimum. If the transmission is discarded due to some reason, sender doubles its contention window and starts retransmission of data.

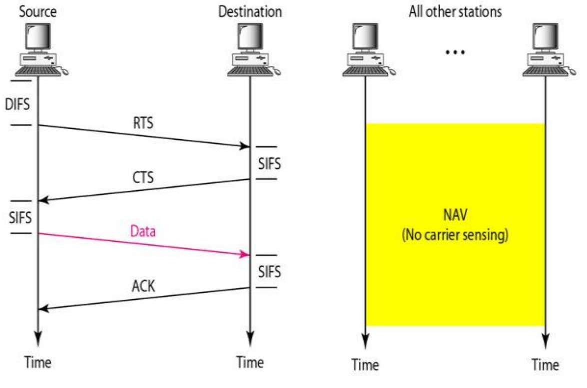


Fig 1: CSMA/CA [7]

If a particular node uses the channel for a long duration and did not give the chance to the other nodes to access the channel, such a node is termed as a selfish node. The objective of selfish node is to degrade the channel performance and impair the overall link efficiency. The selfish node manipulates the following parameter to enhance the channel access probability.

- Selfish node increases the transmission duration of RTS and data frame in order to access channel for a long time and prevents other nodes from accessing the channel.
- Selfish node selects a smaller SIFS duration in order to complete transmission early and immediately initiates the next transmission.
- Selfish node selects a small back off and DIFS duration in order to increase the channel access probability.

While manipulating back off time, selfish node uses the following strategies:

1. **Ingenuous Strategy:** In this strategy selfish node selects a small constant value as its back off time and pretends itself naïve.
2. **Arbitrary Strategy:** In this strategy selfish node selects a random value from contention window as its back off time. Selfish node makes sure that selected back off time is smaller than the normal node’s back off time hence increasing access frequency.
3. **k- Insistent strategy:** In this strategy selfish node doubles its contention window during retransmission. Hence, its back off time is selected by multiplying the randomly selected back off time and k.

The defense scheme is designed by analysing the above mentioned selfish strategies to counter the selfish misbehavior. The detection and defense scheme is carried out by the neighbour node of the selected node.

3.2 Basic Architecture

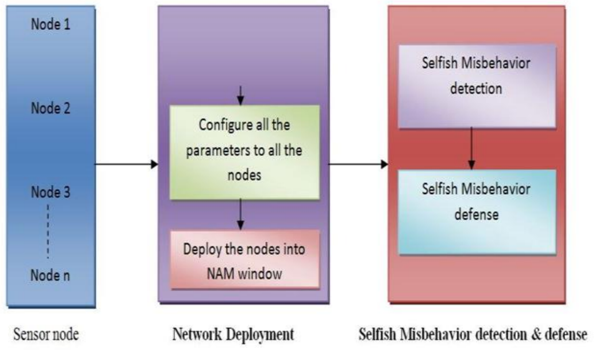

Node 1
Node 2
Node 3
Node n
Configure all the parameters to all the nodes
Deploy the nodes into NAM window
Selfish Misbehavior detection
Selfish Misbehavior defense
Sensor node
Network Deployment
Selfish Misbehavior detection & defense

Fig 2: Basic Architecture of Detection and Defense

The fig 2 depicts the basic architecture of the defense and detection mechanism deployed to safeguard against the selfish misbehavior. Initially all the nodes are deployed. The parameter for the all nodes are configured, viz. multi-hop, initial energy, MAC, propagation time, receiver power, sleep power, transmission power, channel type. Above parameters will be monitored continuously in the NAM window. All nodes will monitor their performance parameters to ascertain the selfish node and employ mechanism for selfish misbehavior. The selfish detection process will determine the selfish node based on RTS and CTS transmission, SIFS and DIFS/back off time manipulation. The defense scheme is employed on detection of the selfish node.

3.3 Detection scheme for selfish misbehavior

Now, it is proposed to detect the selfish misbehavior through the observation of normal nodes. Here, it is considered to take up the case of multi-hop network on the single channel, where each node is under observation by other neighbouring nodes. The data observed by the neighbouring nodes is used for the determination of selfish misbehavior under normal protocol operation. In the IEEE 802.11 network, selfish node can manipulate the four MAC parameters in order to achieve higher channel access probability i.e. transmission of RTS and CTS duration, SIFS duration, DIFS duration and back off time.

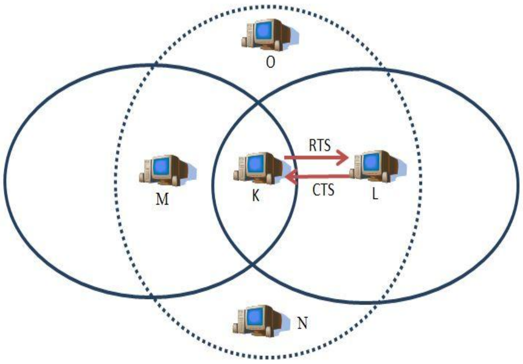


Fig 3: Network topology illustrating the transmission of RTS and CTS

3.3.1 Transmission of RTS and CTS duration for manipulation detection

According to fig 3, K is an observed node and L to O are the neighbouring nodes or observers. In this case M takes a larger value of RTS and data packet duration in order to access channel for long duration. The duration of RTS and data packets are denoted by T_{rts} and T_{data} respectively. When K's neighbour nodes hear data packets it determines whether K is selfish or not by calculating the parameters discussed below.

$D_r = T_{rts} – 3 * SIFS - D_{cts} - T_d - D_{ack}$ (3.1) [8]

$D_d = T_{data}- SIFS - D_{ack}$ (3.2) [8]

Where, D_{cts}, D_{ack} and T_d are the duration of CTS, acknowledgement and data respectively. If D_r (RTS duration) > 0 or D_d (data packet duration) > 0 then K is a selfish node.

3.3.2 SIFS manipulation detection

In this case, selfish node selects a smaller SIFS duration in order to complete transmission early and immediately initiates the next transmission. Then node L to O can infer K's SIFS duration as follows:

$T_s = t_d – t_r - T_r – SIFS - D_{cts}$ (3.3) [8]

Where, t_d and t_r are the duration in which L to O starts hearing RTS and data packet from K. T_r is the duration of RTS. If $T_s <$ SIFS, then K is a selfish node.

3.3.3 DIFS/back off time manipulation detection

Back off time manipulation is difficult to detect in comparison to previous two cases because back off time is a random variable. Since, the normal node selects a random variable as its back off time denoted by B from a contention window W. The probability of node's B is less than or equal to the estimated back off time EB is

$$P [B \leq EB] = \frac{EB+1}{W}$$ (3.4) [8]

Where, P denotes the probability. The above probability itself a random variable denoted by R. if the node is not selfish the expectation of R is

$$E[R] = \sum_{EB=0}^{W-1} \left(\frac{EB+1}{W}\right) \cdot \frac{1}{W} = \frac{W+1}{2W}$$ (3.5) [8]

Where, E denotes the expectation. R is a random variable i.e. it is difficult to determine a node is selfish or not using one sample of R. Therefore, instead of using one sample, the above expression is extended to observe multiple samples of R for different data packets.

Let us consider m as a chosen sample. The detecting back off time and size of contention window for i^{th} $(1 \leq i \leq m)$ sample is denoted by b_i and W_i respectively.

$$R_i = P [B_i \leq b_i] = \frac{b_i+1}{W_i}$$ (3.6) [8]

R_1……R_m is the joint cumulative distribution function denoted by Z. If an observer detects that

$Z \leq \alpha E [Z]$ (3.7) [8]

Then, the considered node is a selfish node, where α $(0 < \alpha \leq 1)$ is a determination factor, the observer detects that the node under observation is a selfish node. Another parameter called trust value is also introduced, to determine the probability of confidence to classify the normal node as a well behaved node. It is denoted by symbol the β and defined as

$\beta = 1 – P [Z \leq \alpha E [Z]] = P [Z > \alpha E [Z]]$ (3.8) [8]

Above mentioned equation is the probability, which states that a node under observation is a selfish node or not. Each one hop neighbour employs above detection scheme and broadcast their result to the local cluster head (chosen by determining the long term behaviour of the nodes). Local cluster head makes a final decision based on the majority in the result.

3.4 Defense scheme

Proposed defense scheme is to defense the smart selfish nodes such as Ingenuous selfish node, Arbitrary selfish node and k-Insistent selfish node from degrading the performance of the normal nodes. These nodes are called smart because they are afraid of detecting due to penalty scheme (reduces the throughput of the detected selfish node). Below mentioned scheme provides guidelines to defend different types of selfish nodes.

3.4.1 Defense scheme for ingenuous strategy

Ingenuous selfish nodes aim is to choose a random time as a back off time in order to access channel for long time compared to normal node. All the one-hop neighbour nodes detection process is based on the determination factor α. Therefore, ingenuous selfish node changes its parameters based on α in order not to be detected by their neighbour nodes as selfish nodes. Ingenuous selfish node back off time is same during multiple samples if all the one hop neighbour nodes of Ingenuous selfish node broadcast constant α. Therefore, ingenuous selfish node can be identified easily by analysing few samples.

3.4.2 Defense scheme for arbitrary strategy

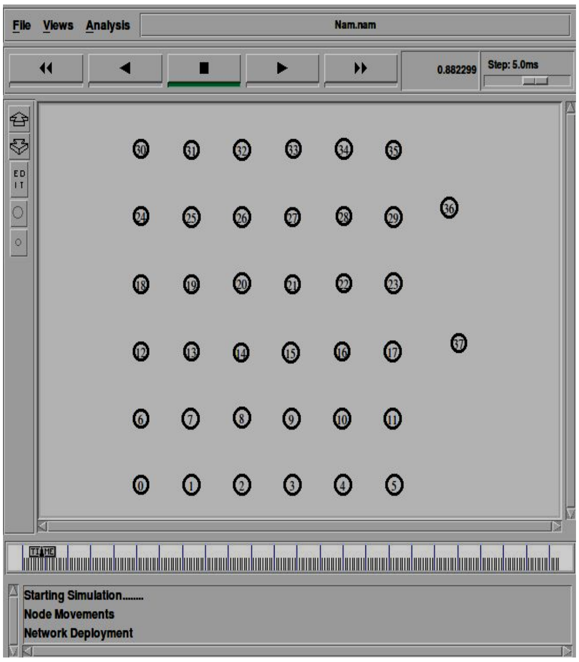
Arbitrary selfish nodes aim is to determine minimum contention window size W_s without being detected by the neighbour node. Arbitrary selfish node determines its back off time uniformly from [0, W_s - 1] by applying Anderson Darling test [9]. It's one hop neighbour nodes determine whether a sample of back off time obeys uniform distribution over the limits [0, W_s - 1]. According to the defense scheme, smallest determination factor α is chosen in order to make selfish node chosen constant contention window size W_s, larger or equal to the expected contention window size of the normal node.

3.4.3 Defense scheme for k-insistent strategy

k- Insistent selfish nodes aim is to choose appropriate k in order to gain higher probability to access channel without being detected by the neighbour node. In k- Insistent strategy, above approach is used for identification of selfish node. Neighbour node best strategy is to employ expected back off time of k- Insistent selfish node not less than the normal nodes.

4. RESULTS AND DISCUSSIONS

The experiments performed with NS2 are described in this section. A network of 38 mobile nodes which are deployed in an area of 650*600 is considered. Initally, all the nodes are configured with parameters such as omni antenna, 802.11 MAC type, wireless channel, two ray ground radio propogation model and the intial energy is set to 100 joules.



Starting Simulation.......
Node Movements
Network Deployment

Fig 4: Network of 38 mobile nodes

4.1 Detection probability

Detection probability is the probability of detecting the selfish nodes from well behaved nodes. Fig 5 shows the proposed simulation system having higher detection probability than that of existing system. In the proposed system, the probability of detecting a selfish node in the network is one in comparison to existing system.

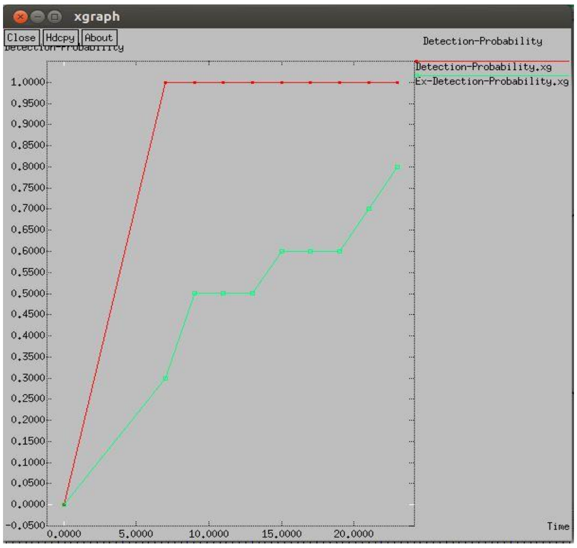


Fig 5: Detection-probability of the proposed system

4.2 Throughput

Throughput is defined as the number of bits per simulation time in milliseconds. Fig 6 clearly shows that the throughput of the proposed system increases in comparison to the existing system.

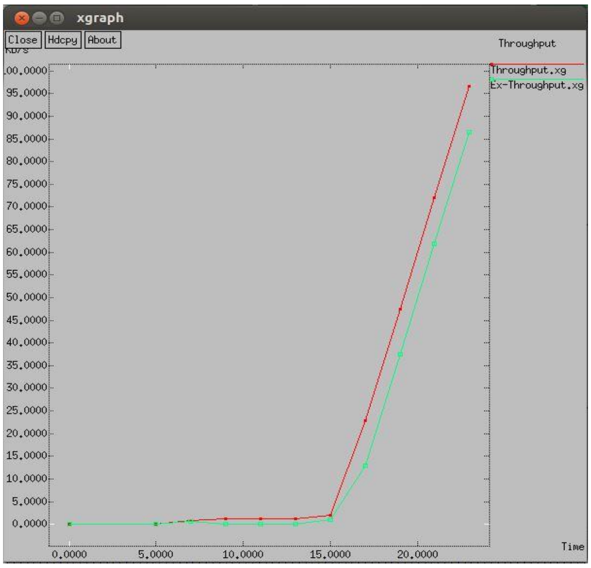


Fig 5: Network throughput of the proposed system

Above, analysis concludes that the proposed system is better than the existing system.

5. CONCLUSION

In ad-hoc network, selfish node can deviate from the regulation and transmit a fake packet to grab the channel for a long time and prevents the well behaved nodes from communicating. In this paper, a detection and defense scheme is proposed which has efficient usage of the network resources and successful delivery of the packets to increase the network performance. Three types of strategy are proposed which provides the guidelines to defend against different types of the selfish nodes. Finally, the above simulation and the results show that the proposed scheme can work well.

6. REFERENCES

[1] V. Gupta, S. Krishnamurthy and M. Faloutsos, “Denial of service attacks at the MAC layer in wireless ad hoc networks,” in *Proc. IEEE Mil. Commun. Conf*., Anaheim, CA, USA, Oct. 2002, pp. 1118-1123.

[2] M. Raya, J. Hubaux, and I. Aad, “Domino: A system to detect greedy behavior in ieee 802.11 hotspots,” in *Proc. ACM 2nd Int. Conf. Mobile Syst., Appl. Serv.*, Boston, MA, USA, Jun. 2004, pp. 84–97.

[3] S. Radosavac, J. S. Babaras, and L. Koutsopoulos, “A framework for MAC protocol misbehavior detection in wireless networks,” in *Proc. 4th ACM Workshop Wireless Security*, Cologne, Germany, Sep. 2005, pp. 33–42.

[4] J. Konorski, “Multiple access in ad-hoc wireless lans with nonco- operative stations,” in *Proc. 2nd Netw. Conf.*, 2002, pp. 1141–1146.

[5] P. Kyasanur and N. Vaidya, “Selfish MAC layer misbehavior in wireless network,” *IEEE Trans. Mobile Comput.*, vol. 4, no. 5, pp. 502–516, Sep. 2005.

[6] Asad Ali, “Improving the performance of the IEEE 802.11 Distributed Coordination Function”, in International Journal of Computer and Communication Engineering, vol. 2, no. 1, pp. 16-19, 2013.

[7] Behrouza A Forouzan and Sophia Chung Fegan,”Wireless LANs”, in *Data Communications and Networking*, 4th edi. New York: McGraw-Hill, 2007, pp. 424–425.

[8] Ming Li, Sergio Salinas, Pan Li, Jinyuan Sun and Xiaoxia Huang, “MAC layer selfish misbehavior in IEEE 802.11 ad hoc networks: detection and defense”, in IEEE transactions on mobile computing, vol. 14, no. 6, pp. 1206–1210, 2015.

[9] T. W. Anderson and D. A. Darling, “Asymptotic theory of certain ‘Goodness of Fit’ criteria based on stochastic processes,” *Ann. Math. Stat.*, vol. 23, no. 2, pp. 193–212, 1952.