Hash Function based MAC Protocol to cope with MAC Layer Misbehavior in Manets

Nagaraju Mopidevi¹, R Madhu²
Department of Electronics and Communication Engineering
JNTU college of Engineering Kakinada, A.P. India
rajmopidevi.in@gmail.com¹
madhu.ramarkula@gmail.com²

Abstract—Mobile adhoc networks consist of mobile nodes connected by wireless links without using any pre-existing infrastructure. MANET nodes rely on network cooperation schemes to properly work, forward traffic unrelated to its own use. However in real world most of the nodes misbehave in order to gain extra bandwidth. Therefore detecting these nodes and providing countermeasure is essential for network performance. This paper proposes a scheme called Hash Function based MAC protocol (HsF-MAC) to cope with backoff cheating technique. HsF-MAC allows MANET nodes to recalculate the backoff value and immediately detect the misbehaving nodes along with effective countermeasure. Moreover colluding behavior (two nodes trying to misbehave collectively) is also detected.

Keywords—MAC layer misbehavior, Backoff cheating technique, MANETS

1. INTRODUCTION
Mobile adhoc networks (MANETS) consists of a collection of mobile nodes which can move freely. These nodes can dynamically self-organize into arbitrary topology networks without a fixed infrastructure. Due to their special characteristics like shared wireless media, limited energy resources, rapidly changing topology MANETS suffer from a range of vulnerabilities. Misbehaving nodes launch a bunch of attacks especially at MAC layer. Misbehaving node disobeys the protocol rules to gain extra bandwidth. It uses several cheating techniques to misbehave; however in this paper we deal with backoff cheating technique in which misbehaving node sets its backoff value to smaller value rather than calculating it following the Binary Exponential Backoff (BEB) algorithm [2]. A simple mobile adhoc network is shown in the figure 1 below. To access the shared media wireless nodes uses IEEE 802.11 protocol [3]. Any misbehavior in accessing the channel alters the network performance. Various approaches have been proposed to design a resistant MAC protocol that is either able to detect or prevent any misuse at MAC level. These approaches can be classified into two categories. The first category of solutions consists of trustworthy central node that monitors the behavior of its neighbor during equal length time intervals and then uses several mechanisms as the work done in [4], [5] to analyze and detect the misbehavior. In the second category backoff algorithm is changed in order to make the backoff value predictable to the receiver. For example backoff value to be used by the sender node is assigned by its intended receiver through a long negotiation process as the work done in [6]. The major drawbacks of these approaches are that they require large number of observation samples to detect the cheaters. Additionally they do not provide countermeasure to cope with collusive misbehavior. To mitigate the above weakness we propose a scheme called Hash Function based MAC protocol (HsF-MAC) to efficiently deal with MAC layer misbehavior launched by both single and colluding nodes. We also propose a reaction scheme to penalize the detected cheaters.
2. PROPOSED SCHEME

The scheme proposed in this paper to deal with MAC layer misbehavior aims to achieve the following one part of communication, detects the nodes which either maliciously chooses small backoff value or refuse to double their contention windows (CW) after collision and ensures fast detection of both single and colluding cheaters. In HsF-MAC two new fields Attempt(Γ) and CRC(Cyclic Redundancy code) are added to each RTS frame where Γ represents number of times the sender has tried to transmit the RTS frame and its corresponding data packet and CRC is Cyclic Redundancy Code calculated over all the fields of data packet to be transmitted. The new format of RTS frame is shown below in figure 2.

![Frame Format](image)

Fig.2. The new format of RTS frame

Using these two parameters we propose a new formula to calculate the backoff value as given below.

\[
\text{backoff} = \text{Hash} \left( \text{fct}(\text{CRC}, \text{Γ}) \mod 2^{\text{Γ}-1} \times \text{cw}_{\text{min}} \right)
\]

Where \( \text{fct}(\text{CRC}, \text{Γ}) = \text{CRC} \oplus \text{Γ} \)

The Γ value is initialized to 1 after a successful transmission and incremented by 1 for each unsuccessful transmission of RTS frame or data packet. CWmin is minimal contention window and varies according to the technology used at physical layer (CWmin = 31 for DSSS). By adopting this scheme the receiver can detect any deviation in backoff value since it is able to recalculate the backoff value chosen by the sender. HsF-MAC guarantees randomness property of regular backoff scheme. The Hash function used refers to one way function like SHA1 and MD5.

The features of HsF-MAC are

- The CRC and Γ values used by the sender to calculate its backoff value are known to the receiver.
- Hash function used prevents any node from setting its backoff to a small value since it is generated by one way function.
- Since value of CRC differs in each packet the fct function used significantly reduces the number of collisions.
- In case if CRC is unchanged during retransmission the new backoff should differ from previous one since Γ value increases for each retransmission.

These features of HsF-MAC make it possible to efficiently detect the node misbehavior. Now we discuss how HsF-MAC detects the cheating nodes.

2.1 Detecting Cheater node.

The receiver node extracts the Γ and CRC values from the received RTS frame and uses them to recalculate the backoff value used by the sender using the formula (1). If the number of idle slots after the last transmission of the sender is less than (backoff + DIFS), this indicates that the sender has violated the protocol thus it deserves punishment. In case of consecutive collisions incurred by the collision of either CTS or data frames a cheater node may follow the backoff computational rule but keeps the Γ value unchanged. HsF MAC easily detects this misbehavior by comparing the CRC values corresponding to respective RTS frames. If these values are equal and Γ is unchanged then it indicates that sender is a cheater. Incase if cheating node alters the CRC to mislead the receiver node a simple comparison of CRC values received and CRC value calculated over the received data frame reveals the misbehavior of cheater node.

2.2 Reaction Scheme: Warn or Punishment

Our reaction scheme gives a chance to the cheating node to obey the protocol rules, so as to avoid being punished. We have chosen this scheme because we believe that it is better to incite a cheater node to behave correctly rather than excluding it from the network. This is because in MANETs, every node contributes significantly to ensure the availability of network’s services such as connectivity, routing and Internet access. If the cheater node is the only node providing connection to some nodes then its exclusion from the network may lead to network partition and unavailability of some services like Internet connection. The punishment may potentially leads to overloading the other nodes if a load balancing mechanism is not in position. One of the main challenges related to cheater nodes advertisement in MANETs is the prevention of false alarms that severely affects the network performance. These false reports are usually issued from adversary nodes claiming that a given legitimate sender does not comply with the protocol, which leads to its exclusion from the network.

If sender node is observed not obeying the protocol rules by its corresponding receiver, the receiver sends a special message, dubbed Warn-single, which advertises the MAC address of the cheater node as well as the observed deviation from the calculated backoff value. The format of this message is shown in Fig. 3. TTL is Time to Live ie, the number of hops the message can travel. This value is chosen sufficient to allow all the neighbors of the cheater node to receive the Warn-single message.

![Packet Format](image)

Fig.3. Warn-Single Packet format
On receiving this message, each node starts monitoring all the transmissions initiated by the advertised node in order to check whether it is correctly applying the MAC protocol rules or not. Here, the dissemination of the sender’s identity is used to warn the sender that its direct receiver has been aware of its misbehavior, so it is urged to change that behavior by calculating the backoff value according to the protocol. If it changes its behavior and obeys the protocol rules, then no punishment will be applied against it, otherwise all its neighbors will punish it. The one hop neighbors of the cheater node would be aware of its misbehavior as follows. The advertiser of the Warn single message sets the TTL value to m which is decreased at each hop. Upon reception of this message, if the receiver node is a neighbor of the cheater node so it discards the message, otherwise it rebroadcasts it (except if the TTL reaches 0). To penalize a confirmed cheater node, each of its neighbors may refuse to respond to its communication requests or delay the delivery of data packets or forwarding of its data packets, which leads to severe performance degradation at the cheater side. Further, those neighbors may also launch a cross layer punishment scheme by refusing to relay any control message sent by the cheater node, so it can never be involved in a routing path.

2.3 Detecting colluding cheaters.

Most of the current countermeasures do not cope with sender-receiver collusion. This misbehavior leads to significant reduction of the throughput acquired by the neighbors of the colluding nodes. To detect this misbehavior, we propose to extend our detection scheme as follows. The node experiencing decrease in throughput monitors the transmissions in its vicinity to identify the nodes getting higher throughput. After identifying those nodes, the monitor node carefully observes every transmission originated from them and checks whether they comply with the backoff computation rules or not. If any node disobeys our proposed scheme and its intended receiver didn’t inform its neighbors about this misbehavior, the monitor node then piggybacks both of their identities in a special message, dubbed Warn collusion, as shown in figure 4 along with the corresponding estimated deviation, which is the difference between the backoff value calculated according to the Equation (1) and the observed one. The receiver identity is also advertised to flag that it refuses to reveal the identity of a cheating node. To detect this misbehavior, the monitor node should be either a neighbor of both the sender and receiver or collaborate with another node such that each of them is a neighbor of one of the cheating nodes.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of nodes</td>
<td>5……150</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Direct Sequence</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250m</td>
</tr>
<tr>
<td>Data Rate</td>
<td>3 mbps</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR(500 bytes per packet)</td>
</tr>
<tr>
<td>Nodes Speed</td>
<td>5 m/s</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>200 seconds</td>
</tr>
</tbody>
</table>

A TTL value is also included in the advertised message in order to make all the neighbors of both nodes aware of their misbehavior. These neighbors will then monitor the behavior of the advertised nodes until either their misbehavior is confirmed or they have repented and complied again with the protocol. If their misbehavior is confirmed then they are penalized as mentioned in section 2.2.

3. PERFORMANCE EVALUATION

To evaluate the effectiveness of Hash function based MAC protocol (HsF-MAC), we have conducted a set of simulations using Network Simulator (NS2). The mobility model is based on two ray ground propagation model in the field of 1000m x 1000m. Wireless nodes are randomly moving, at a speed of 5m/s within the network topology and exchanging 500 bytes CBR packets. We use SHA1 (160bits) as a hash function to implement HsF-MAC. Simulation time for each simulation scenario is set to 200 seconds. The setting of the simulation parameters is summarized in the Table 1.

After simulation the network animator output for the proposed protocol will be as shown below. Fig.5 shows layout of nodes in the wireless network before transmission of information. Fig.6 refers to propagation of all nodes and coverage of nodes at sometime. Fig.7 refers to the transmission of packets from source to destination. Here the source is from node 7 and destination is node 12. The Fig.8 shows that the packets are dropped at some nodes.
The performance of Hash function based MAC protocol (Hsf-MAC) protocol is evaluated using following performance metrics:

**Packet Delivery Ratio:** Packet delivery ratio is defined as the ratio of number of data packets successfully received by CBR destinations to the number of data packets generated by the CBR sources. Fig. 9 shows the effect of packet interval on packet delivery ratio. As number of packets per second increases packet delivery ratio decreases. Packet delivery ratio is high after detecting the misbehaving nodes. We can see the deviation of performance without and with detection of misbehavior nodes. Packet delivery ratio is high after detecting the misbehaving nodes.

**Throughput:** Total number of delivered data packets divided by total duration of simulation time is throughput. We analyze the throughput in terms of messages delivered per second. Fig.10 shows the effect of packet interval on the throughput without detection and after detection. It shows that the throughput increases after detection of misbehaving nodes.

**Dropping Ratio:** The number of packets dropped during transmission is dropping ratio. The variation of dropping ratio with respect to packet interval without and with detecting the misbehaving nodes is shown below. Fig.11 shows that the dropping ratio is decreased after detecting the misbehaving nodes and providing countermeasure.
Normalized routing overhead: Normalized overhead is defined as the ratio of total packet size of control packets to the total packet size of data packets delivered to the destination. Figure 12 shows the variation of normalized routing overhead with varied packet interval and before and after detecting misbehavior nodes. Normalized routing overhead is less after detecting the misbehaving nodes.

Delay: The average delay of successfully delivered CBR packets from source to destination node. The variation of delay with respect to packet interval is shown in the figure below. In some case delay will be more after detection.

4. CONCLUSION

We have designed a new backoff scheme to quickly detect the cheating nodes that do not obey the MAC layer protocol. This Hash function based MAC protocol (HsF-MAC) is able to identify the nodes that do not calculate backoff value properly after one successful transmission of an RTS frame or its corresponding data packet. Therefore, the impact of the cheater node on the bandwidth fair-share is counteracted efficiently. The HsF-MAC also detects sender-receiver collusion. It ensures fair share of bandwidth. In addition, a reaction scheme is proposed to penalize the detected cheaters. Our reaction mechanism allows the cheaters to become honest rather than punishing them. This is achieved through the warning message disseminated by the detector node, which constitutes double notification. It warns the cheater node regarding its misbehavior and discloses its identity to its neighbors. So, the cheater node will either stop its misbehavior to avoid punishment or keep it until being punished by the neighbors.

REFERENCES


