Handling MAC Layer Misbehavior in Wireless Networks

Pradeep Kyasanur
Dept. of Computer Science, and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
kyasanur@crhc.uiuc.edu

Nitin H. Vaidya
Dept. of Electrical and Computer Eng., and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
nhv@crhc.uiuc.edu

Categories and Subject Descriptors

C.2.0 [**General**]: Security and Protection; C.2.3 [**Network Operations**]: Network Monitoring

General Terms

Security

Keywords

Wireless security, Misbehavior detection

1. INTRODUCTION

Wireless MAC protocols such as IEEE 802.11 use co-operative contention resolution mechanisms for sharing the channel. In this environment, some *selfish* hosts in the network can misbehave by failing to adhere to the network protocols with the intent of obtaining an unfair share of the channel bandwidth. Our work focusses on detecting and handling MAC layer misbehavior by *selfish* hosts in IEEE 802.11-based networks.

In IEEE 802.11 DCF mode, nodes exchange RTS and CTS packets to reserve the channel before data transmission (When data packets are small RTS/CTS exchange may be omitted.) A node with a packet to transmit picks a random backoff value b chosen uniformly from range [0,CW], where CW is called the Contention Window, and transmits after waiting for b idle slots. If a transmission results in a collision, the CW value is doubled. The throughput obtained by a node is inversely proportional to the average time it waits in backing off. So, misbehaving nodes can obtain a higher share of throughput by selecting small backoff values or by not doubling the CW value after a collision.

2. HANDLING MISBEHAVIOR

Random selection of backoff values allows a node to select a sequence of small backoff values. This prevents easy detection of misbehavior as misbehaving nodes may appear to have legitimate behavior in the short-term. One can use traffic analysis to identify nodes which seem to be obtaining more than their fair share of bandwidth. However, it is difficult to decide the *fair* share of bandwidth a node should receive because of the inherent unfairness of IEEE 802.11 protocol. Statistical methods like traffic analysis can only detect node misbehavior occuring over a reasonably long interval of time. Consequently, short-term misbehavior may not be detected. A misbehaving node can also achieve lower average delay compared to a conforming node even when misbehaving for short intervals at a time. If the traffic is mostly bursty, then the misbehaving node can transmit the burst of packets by selecting small backoff values, with low delay. Traffic analysis may not catch this type of behavior. In [1], game-theoretical analysis has been used to develop a backoff procedure that attempts to ensure *fair* share of bandwidth to well-behaved nodes.

An alternate approach that we adopt is to modify the MAC protocol to use a deterministic backoff procedure, allowing better monitoring of the node behavior.

Detection Procedure: We present a detection procedure for a network having a single well-behaved receiver and multiple potentially misbehaving senders. An example of this is an infrastructure-based network having a well-behaved base station (receiver) and multiple mobile hosts (senders). Mobile hosts communicate only with the base station. We present our solution with this example of infrastructure-based networks. However, this solution can be applied for ad hoc networks as well.

The base station provides the backoff value to be used by a host for its $(i+1)^{th}$ transmission in the CTS or ACK packet of the i^{th} transmission. The base station can then count the number of idle slots between i^{th} and $(i+1)^{th}$ transmission from the host (by monitoring the channel) and verify that the host has at least waited for the required number of idle slots. On collision, the host generates a new backoff value using a deterministic function f as follows,

$$\text{Next backoff} = f(\mathit{initialBackoff}, hostId, attemptNum)$$

The host also includes the retransmission number in every attempted transmission. When the base station successfully receives a packet, it computes the expected amount of time the host should have waited using the knowledge of the transmission attempt number, host identifier and the

MOBICOM'02, September 23–28, 2002, Atlanta, Georgia, USA.

originally assigned backoff value as follows

$$S_{expected} = \sum_{i=1}^{attemptNum} f(initialBackoff_T, hostId, i)$$

The base station maintains a counter to count the idle slots on the channel. The base station stores the idle counter value at the end of a successful transmission from each node. When the next transmission from that node is received, the difference in the stored idle counter value and the current idle counter value gives the estimate of the actual number of slots (S_{actual}) waited by the host. The node behavior is deemed to be deviating from normal if,

$$S_{actual} < \alpha * S_{expected}, \text{where } 0 < \alpha \leq 1$$

When the above condition is true, the node is designated to have *deviated* from the protocol. If K deviations are identified in a window of *THRESH* packets from the node (α,K and *THRESH* are protocol parameters), it is designated to be *misbehaving*. Inaccuracies in monitoring arise when the receiver and the senders have a different view of the channel status. In particular, when the sender senses the channel to be idle while the receiver senses the channel to be busy, the estimated S_{actual} may be smaller than $S_{expected}$, leading to incorrect designation of the host as misbehaving. The misprediction percentage depends on the variations in channel conditions.

Correcting Misbehavior: The mechanism we have presented above allows for detecting misbehaving nodes with high accuracy. The next step is to explore MAC layer mechanisms for handling misbehavior. The benefits gained by misbehaving nodes are increased throughput and decreased delay. Thus, the aim of the "correction" mechanism is to negate the benefit gained by the misbehaving nodes while not penalizing the conforming nodes.

When the monitoring procedure detects that a node has waited for less than the assigned backoff for the current transmission by an amount D, this amount D is added as penalty to the next backoff assigned to that node. This procedure reduces the throughput advantage gained by the misbehaving nodes. However, it is not completely successful in negating the advantage of misbehaving nodes as they benefit from having lesser collisions on an average for every successful transmission. For example, consider a network having only two nodes A and B. Node A misbehaves by transmitting packets at a higher rate than the well-behaved node B. Then, the total collisions suffered by both the nodes is the same, but the number of collisions per successful transmission is less for the misbehaving node as it transmits more often. Hence, the average backoff for the misbehaving node is lesser than that of the well-behaved node. We have done simple theoretical analysis to estimate the benefit gained by misbehaving nodes from reduced collisions. We compute this benefit from reduced collisions and add the amount as additional penalty to the backoff value of the node in the subsequent transmission.

3. SIMULATION RESULTS

We use *ns-2* simulator for our simulations. The details of the simulation model and results are presented in [2]. Preliminary results indicate that fairly accurate misbehavior detection is possible. Using MAC layer misbehavior correction appears to be successful in restricting the bandwidth share obtained by misbehaving nodes to that obtained by well-behaved nodes. Fig. 1 compares the throughput obtained by a misbehaving node with and without the *correction* scheme. The simulation setup has 8 nodes placed equally apart in a circle around the base station and one randomly selected node is misbehaving. The misbehaving node backs off for a fraction of the assigned backoff and this fraction is designated as "Percentage of Conformance". "AVG TPUT" is the average throughput obtained by the nodes in the network. "MSB TPUT" is the throughput obtained by the misbehaving node. Details of other parameters in the figure are omitted here for brevity. The throughput obtained by the misbehaving node is close to the average throughput (which is an estimate of the *fair* share), when *correction* scheme is used.

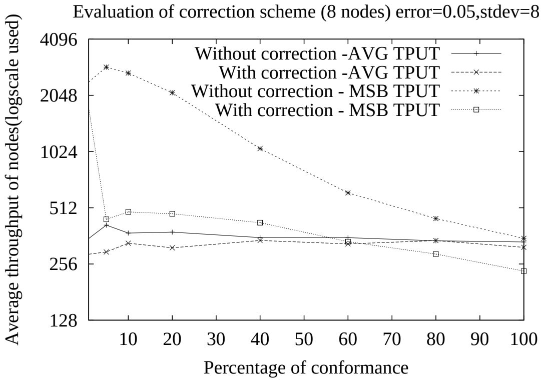

Figure 1: Comparison of average and misbehaving node throughput with and without correction

4. CONCLUSION AND FUTURE WORK

Handling MAC layer misbehavior is an important requirement in guaranteeing service availability. In this paper, we have presented a MAC protocol which simplifies misbehavior detection for a scenario having single well-behaved receiver and multiple senders. The approach can be used in ad hoc networks as well. Each node in the ad hoc network monitors the traffic it receives to verify that the nodes sending the packets are well-behaved. We plan to augument our approach with mechanisms to detect a misbehaving node that gains more bandwidth by using multiple MAC addresses. We plan to develop and evaluate protocols for handling misbehavior for scenarios having misbehaving receivers and scenarios with colluding senders and receivers. We will also explore other approaches for detecting and correcting misbehavior.

5. REFERENCES

[1] J. Konorski. Multiple Access in Ad-Hoc Wireless LANs with Noncooperative Stations. In *Proceedings of NETWORKING 2002*, vol. 2345 of *LNCS*. Springer, 2002.

[2] P. Kyasanur and N. H. Vaidya. Detection and Handling of MAC Layer Misbehavior in Wireless Networks. Technical report, CSL,UIUC, August 2002.