Detection of Misbehaviour at Mac Layer in Wireless Networks

Omkar Nath Tiwary

Abstract— the IEEE 802.11 CSMA/CA protocol is most commonly used MAC protocol for wireless network. This protocol is used to access the media. But IEEE 802.11 works properly only if all the stations obey the MAC protocol. Some node can substantially increase his share of bandwidth by slightly changing the parameters of MAC protocol, in order to increase their throughput. This cause throughput degradation of all well behaved node. In this paper, we proposed the detection scheme for such misbehavior at MAC layer in wireless networks.

Keywords—MAC-misbehaviour, RTS re-transmission rate, throughput, back off value

1. INTRODUCTION

The IEEE 802.11 is a standard for a wireless LAN covering both physical and MAC layers. The IEEE 802.11 MAC protocol provides two service types of service: asynchronous and synchronous (or, rather, contention free).

The asynchronous type of service is provided by the Distributed Coordination Function (DCF) which implements the basic access method of the IEEE 802.11 MAC protocol and is also known as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. This IEEE 802.11 CSMA/CA [13] protocol is used for sharing the wireless channel among the various nodes.

The contention resolution mechanism depends on inherent trust among nodes. In environments where hosts in the network are untrusted, some hosts may misbehave by failing to adhere to the network protocols, with the intent of obtaining an unfair share of the channel.

In such an environment, by simply manipulating the back-off timers and/or wait times prior to transmission, such nodes can cause a drastically reduced allocation of bandwidth to well behaved nodes.

2. IEEE 802.11 DISTRIBUTED CO-ORDINATION FUNCTION (DCF)

According to the DCF a station must sense the medium before initiating the transmission of a packet. If the medium is sensed as being idle for a time interval greater than a Distributed InterFrame Space (DIFS) then the station transmits the packets. Otherwise, the transmission is deferred and the backoff process is started. Specifically, the station computes a random time interval, the backoff interval, uniformly distributed between zero and a maximum called Contention Window (CW). This backoff interval is then used to initialize the backoff timer. This timer is decreased only when the medium is idle, whereas it is frozen when another station is transmitting. Specifically, each time the medium becomes idle, the station waits for a DIFS and then periodically decrements the backoff timer. The decrement period is referred to as the slot-time which corresponds to the maximum round-trip delay within the maximum wireless range of the network. As soon as the backoff timer expires, the station is authorized to access the medium. Obviously, a collision occurs if two or more stations start transmission simultaneously. Unlike wired networks (e.g., with CSMA/CD), in a wireless environment collision detection is not possible. Hence a positive acknowledgment is used to notify the sending station that the transmitted frame has been successfully received. The transmission of the acknowledgment is initiated at a time interval equal to the Short InterFrame Space (SIFS) after the end of the reception of the previous frame. Since the SIFS is, by definition, less than the DIFS the receiving station does not need to sense the medium before transmitting the acknowledgment. If the acknowledgment is not received the station assumes that the transmitted frame was not successfully received and, hence, schedules a retransmission and, the backoff process starts again. However, to reduce the probability of collisions, after each unsuccessful transmission attempt, the Contention Window is doubled until a predefined maximum (CWmax) is reached. After a (successful or unsuccessful) frame transmission, if the station still has frames queued for transmission; it must execute a new backoff process

- *Omkar Nath Tiwary are currently working as a lecturer in Information Technology in St.Joseph College of Engineering and Technology, Tanzania.*
Mobile: +255 687450588, +255 659513899.
E-mail: tiwary45@gmail.com.

3. MAC LAYER MISBEHAVIOR

IEEE 802.11 MAC protocol favors the node that selects the smallest back-off value among a set of contending nodes. Therefore, such node may choose not to comply with protocol rules by selecting small back-off intervals to gain significant advantage in channel sharing over well-behaved nodes. Moreover, due to the exponential increase of the contention window after each unsuccessful transmission, well-behaved nodes will select their backoff value from larger intervals after every collision. Therefore, the chance of their accessing the channel becomes even smaller. Apart from intentional selection of small back-off values, a node can deviate from the MAC protocol in other ways as well. It can choose a smaller contention window or he may wait for an interval shorter than DIFS(Distributed inter frame space), or reserve the channel for an interval larger than the maximum allowed NAV (Network Allocation Vector) duration.

4. Related Work

Many misbehavior detection approaches are proposed for detecting such behavior in network traffic but selfish or greedy behavior of nodes at MAC layer remains a hard to resolve this problem. Some of the flaws in these schemes are:

[2] Requires a modification of the IEEE 802.11 MAC protocol in a way that is incompatible with the current standard. Such an approach is practically unfeasible.

[7] Gives control to the receiver over the sender, by making the former assign backoff values to the latter in both the detection and the correction schemes. Hence the proposed approach opens the door to new misbehavior techniques, including misbehaving receiver and collusion between sender and receiver.

[2] Creates communication and computation overhead. The first is due to the addition of new frame header fields and the second to the detection and correction schemes that have to compute backoff and, in some cases, penalties for each individual frame of the sending station (in the infrastructure case, all this load will be centralized at the AP).

DOMINO[4] fails to detect an adaptive cheater which alternates randomly among several misbehavior techniques in order to evade detection.

Konorski [5] considers an ad hoc network in which all stations hear each other and he proposes a misbehavior-resilient backoff algorithm based on game theory. As it requires a new backoff mechanism, different from the current standard, this solution is not practical for current hotspots.

In [10] a new class of protocol-compliant attacks, timeout attack, has been presented to disrupt packet forwarding, thereby defeating a Watchdog-like detection system deployed at the MAC layer. This type of attack can deliberately delay the transmission of MAC frames, such as RTS and DATA, by a minimum required time. Consequently, a malicious node can force a well behaved node to drop the packets at the MAC layer while the malicious node itself completely follows the protocols, thus hiding from the Watchdog detection system.

The common disadvantage of the herein described solutions is that either, it requires a modification of IEEE 802.11 MAC protocol or, it creates communication and computation overhead. So this type of approach is practically unfeasible.

5. Simulation Software

We use the network simulator (NS3) [14] for our simulations. We first created the network topology by creating subnets, placing nodes, defining node mobility and configuring the general properties of the network

6. Scenario Description

We have used eight nodes numbered form 1, 2, 3….8. In which node 1 is the Access Point (AP). All eight are working under Wireless Network using AODV (ad hoc on-demand distance vector) routing protocol. All the nodes are using IEEE 802.11 MAC protocol.

a. Simulation of wireless network without MAC misbehavior

In this scenario, all nodes (1, 2, 3….8) are using same 802.11 MAC protocol.

b. Simulation of wireless network with MAC misbehavior

In this scenario also, all nodes are using 802.11 MAC protocols except node 3 and 6 which are behaving as MAC misbehaving node and communicating with each other through ALOHA as a MAC protocol. These two nodes, which are using ALOHA as MAC protocols will behave like the misbehaving nodes on the scenario and decrease the throughput as well as increase the packet drop ratio of all other well behave nodes by making the channel busy for other nodes. So that the number of RTS retransmission due to such behavior increases in the network.

7. Detection Scheme

In this detection scheme, first of all collect the statistical values of all nodes RTS retransmission due to time out, packet retransmission due to ACK timeout and throughput at receiver end then compare it with the threshold value. If the value is above the threshold value for RTS and packet retransmission as well as below the threshold value for throughput then selfish attack is occurring otherwise scenario is not containing any selfish nodes all are working properly without any selfishness.

In Figure 1, 2 and 3, the statistical results show the comparative study of Throughput, RTS retransmission rate and packet retransmission rate of nodes under well behaved and selfish attack.

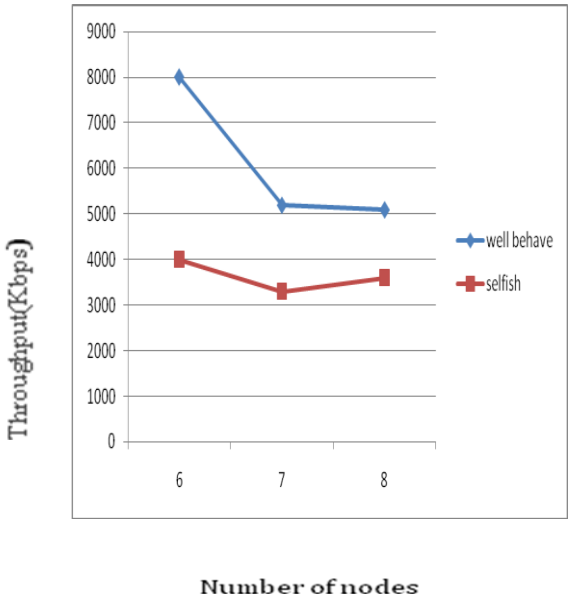

Figure 1:Throughput comparison

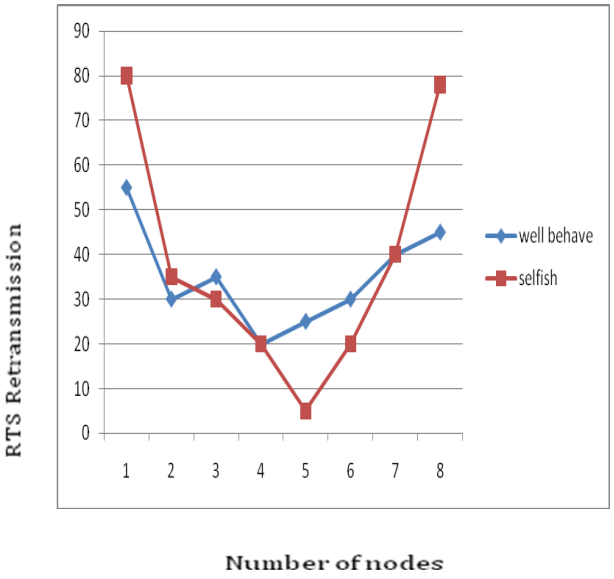

Figure 2: RTS retransmission rate comparison

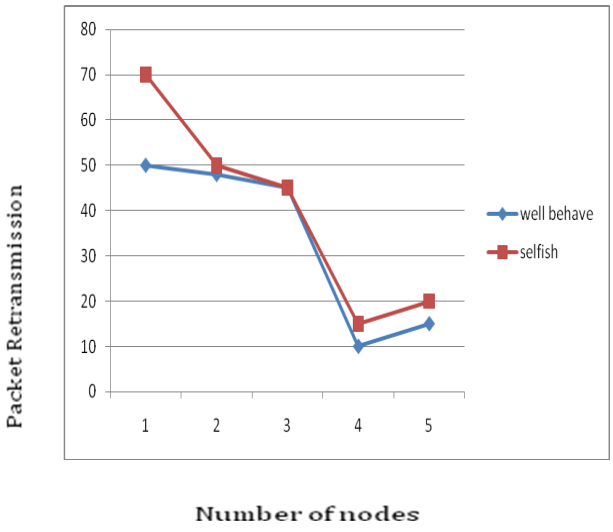

Figure 3: Packet retransmission rate comparison

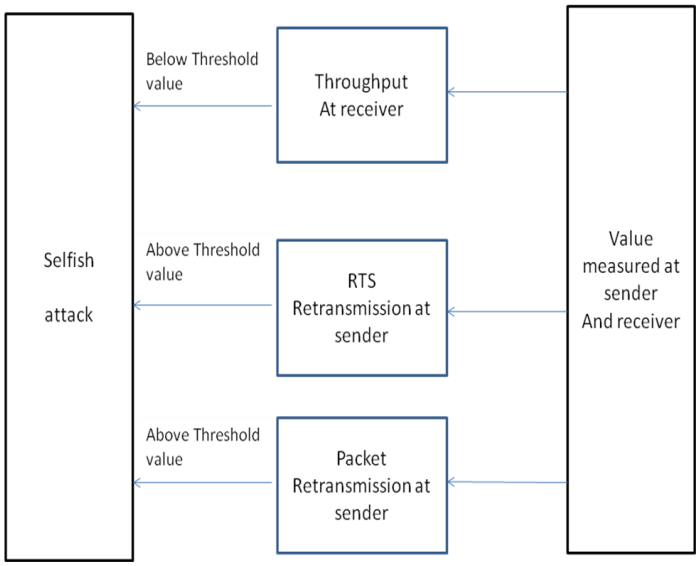

Figure 4: Detection scheme for selfish MAC misbehavior

8. ACKNOWLEDGMENT

I have taken efforts in this journal. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend my sincere thanks to all of them. I am highly indebted to Directors, principal, and member of St.Joseph College of Engineering and Technology, Dar Es Salaam, Tanzania for their guidance and constant supervision as well as for providing necessary information regarding the Journal and also for their support in completing the Journal. I would like to express my gratitude towards my parents.

9. CONCLUSIONS

The statistical results show that the selfish node has increased the RTS retransmission rate and packet retransmission rate of well behaving nodes, whereas throughput degrades under selfish attack. Our proposed detection scheme for such MAC misbehavior in the scenario detects this attack by considering these parameters at both ends.

REFERENCES

[1] Y.-C. Hu and A. Perrig, "A survey of Secure Wireless AdHoc Routing",IEEE Security & Privacy, Special Issue on Making Wireless Work, May/June 2004.

[2] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," IEEE Trans. Mobile Computing, Sept. 2005.

[3] [3] V. Gupta, S. Krishnamurthy, and M. Faloutsous, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," Proceedins of MILCOM, 2002.

[4] M. Raya, J. P. Hubaux, and I. Aad, "DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots," IEEE Transaction Mobile Computing, 2006.

[5] J. Konorski. "Multiple access in ad hoc wireless LANs with noncooperative stations". In NETWORKING, volume 2345 of LNCS, Springer, 2002.

[6] R. Jain, G. Babic, B. Nagendra and C. Lam, "Fairness, Call Establishment Latency and Other Performance Metrics", Technical Report ATM Forum/96-1173, ATM Forum Document, Aug. 1996.

[7] C. He and J. C. Mitchell, "Analyzing and Improving the IEEE 802.11 MAC Protocol for Wireless LANs," Proceedings of NDSS, Feb. 2005.

[8] A. Cárdenas, S. Radosavac, and J. S. Baras, "Detectionand Prevention of MAC Layer Misbehavior for Ad Hoc Networks," ACM SASN, Oct. 2004.

[9] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions",USENIX Symposium., 2003.

[10] L. Guang and C. Assi, "A Self-Adaptive Detection System for MAC Misbehavior in Ad Hoc Networks," Proceedings of IEEE ICC, June 2006.

[11] L. Guang, C. Assi, and A. Benslimane, "Modeling and Analysis of Predictable Random Backoff in Selfish Environments," Proc. ACM/IEEE MSWiM, Oct. 2006.

[12] S. Djahel and F. Na Abdesselam, " FLSAC: A New Scheme to Defend Against Greedy Behavior in Wireless Mesh Networks", International Journal of Communication Systems (IJCS), Wiley InterScience Publisher, 22(10):1245-1266, june 2009.

[13] IEEE Standards for Wireless LAN-Medium Access control and Physical Layer Specification, P802.11, 1999.

[14] *NS3 home page. [Online Available] http://www.nsnam.org/.*