RESEARCH REVIEW JOURNALS
Volume-03
Issue-07
July-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Mitigating Selfish Misbehavior Attack in MANET by SMD Algorithm

*A. Priyadharshini

Assistant Professor, Department of Information Science and Engineering, CMR Institute of Technology, Bangalore (India)

ARTICLE DETAILS

Article History
Published Online: 05 July 2018

Keywords
Selfish Misbehavior, Channel Allocation, Attacks, Cluster Head

***Corresponding Author**
Email: priyacse6[at]gmail.com

ABSTRACT

MANET is a self-organized and decentralized wireless network, which is widely used in military applications, game parties, conferencing, etc. Due to its dynamic topology MANET is highly exposed to wide variety of attackers. Selfish misbehavior in channel allocation is a type of passive attack that affects the data link layer which will harm the network severely. As selfish misbehavior is a passive attack it is very difficult to detect. In this paper, Selfish Misbehavior Detection (SMD) algorithm is proposed that detects the selfish misbehavior during channel utilization. The mechanism uses cluster head for both detection and penalization. In every attack, detection process there is a possibility for false positive and false negative. In order to overcome this pitfall crosschecking mechanism is also integrated with the detection process. The proposed scheme not only simply detects the selfish behavior but also penalizes the selfish node.

1. Introduction

MANETs – Mobile Adhoc Networks are type of wireless networks which don't have any fixed infrastructure. This type of network doesn't have any centralized administrator, i.e. every node in the network is autonomous in nature. As MANET is easy to deploy, it is used in military applications and disaster operations. MANET is also having lot of constraints such as battery power, low coverage area, movement of nodes, security issues and so on. Every node in the network acts as a router. So any node can send data to any other node at any time. As MANET is dynamic in nature, any node can enter the network at any time and any node can also leave the network at any time. It is very tedious to monitor the routing table. The basic functionality of any secure computing/networking is to ensure confidentiality, availability and integrity of data.

In MANET lot of security constraints are there, especially channel allocation is a critical issue. Without proper channel allocation mechanism collision will occur, i.e. if many nodes access the same medium at same time then collision will occur. So proper channel allocation strategy need to be deployed. If a node is out of the other nodes transmission range then two nodes will send data to a node at same time. Such that the receiver nodes end will get collided.

Three types of assignment schemes have been used in any wireless network. The schemes are,

1. **Fixed assignment scheme:** The channel is assigned based on time, frequency and codes in fixed manner. This scheme is further divided into frequency division multiple access, time division multiple access and code division multiple access.

2. **Random assignment scheme:** The channel is allocated in random manner along with time slots. This scheme is further divided into aloha and slotted aloha.

3. **Reservation based scheme:** The sender will reserve the medium by sending RTS (Request to Send) and then will start sending the data if it receives corresponding CTS (Clear to Send). These schemes can be deployed in the MANET too as it is also one type of wireless network. But there is also another issue in MANET that need to be considered. The issue is security. Due to the dynamic topological nature MANET often suffer from security threats. As one can enter and leave the network at any time, it is very simple and easy for the attacker to launch the attack.

2. Attacks

In every network the attacks can be broadly classified into active and passive attacks which in turn have subtypes as depicted in Table 1. As there is only wireless links between nodes, MANET is easily susceptible to all types of attacks. Attacks can be broadly classified into active and passive attacks.

In Passive attack, the attacker will simply get the information, utilize the resources but won't try to alter anything. In active attack, the attacker will try to insert, delete and modify the data. As in active attack the attacker activity can be easily identified, it is very difficult to identify a passive attacker.

Table 1 Classification of Attacks in MANET

S. No.	Types of Attack	Subtypes of Attack	
1	**Passive Attack**	Eavesdropping, Selfishness	
2	**Active Attack**	Layers	Attacks
		Application Layer	Repudiation
		Network Layer	Black hole, Wormhole, Byzantine, Routing attack, Information disclosure
		Transport Layer	Session hijacking, SYN Flooding

		Data Link Layer	DOS, MAC, Targeted attack
		Physical Layer	Jamming, Device Tampering
		Multi-Layer	Man in middle attack, DOS, Impersonation

In Data link layer selfish misbehavior is a major concern, because the attacker node will utilize the channel for long time, so that, the channel can't be accessed by the normal nodes. In this case, the traditional assignment schemes won't be used because it can't handle selfish misbehavior. In order to handle this selfish behavior attack an efficient mitigation/channel allocation scheme with misbehavior handling capability need to be deployed. Traditional cryptographic techniques such as encryption and decryption won't be deployed in the data link layer. So, an intelligent or efficient technique need to be deployed that should handle both channel allocation and selfish misbehavior.

3. Related Work

Many of the traditional selfish misbehavior detection mechanisms available so far are applicable only for wireless local area network. Those mechanisms may either use historical data or delay and throughput models for detection, which are applicable only for wireless Local Area Networks. In the paper [21], a real time selfish misbehavior detection mechanism has been proposed for Mobile Adhoc Network. The mechanism requires only few samples for detection of selfish misbehavior and also adaptable to the dynamic nature of channel allocation. This detection methodology protects the selfish node to degrade the performance of normal nodes. A lite weight dynamic channel allocation with corporative load balancing approach has been proposed, whereas channel handover has not been handled.

In 802.11, Carrier Sense Multiple Access (CSMA/Collision Avoidance) has been deployed, where the network can be accessed in a corporative manner with a random waiting time [1]. In MANET, as there is no centralized administration the malicious node can access the channel for a long time such that the normal nodes can't access the medium [4] [6].

Modification had been made to the 802.11 protocol to facilitate detection of selfish misbehavior. In this detection the receiver assigns the back off timer to the sender if the sender deviates from the back off timer, the receiver will penalize the sender by reducing the back off timer, Such that the sender will get only small back off timer. If the sender still deviates, the receiver will identify the sender as selfish node [8] [10]. But this detection scheme would not suit for the dynamic topology like MANET [12] [14].

Game theoretic techniques which impose adequate costs on network operation can also been used to detect selfish misbehavior [15] [16]. A Markov chain based model has been used to detect real time misbehavior [17]. In this technique every node accesses a channel by using the probability determined by the contention window size. In fixed channel allocation, the channel is allocated to the nodes based on fixed manner. This fixed allocation mechanism suits only for uniform traffic. To overcome this dynamic channel allocation has been proposed. Comparison of fixed channel allocation and dynamic channel allocation has been discussed [19].

A coordinated MAC protocol named MH-TRACE (Multi-hop time reservation using adaptive control for energy efficiency) in which cluster head is dynamically chosen for regulating channel access, but it doesn't supports channel borrowing mechanism and hence not suitable for non-uniform load distribution. In order to overcome this DCA-TRACE (Dynamic channel allocation for trace) has been proposed, which is used for both uniform and non-uniform traffic loads [18]. A dynamic cluster based channel allocation mechanism have been used which incorporates cooperative load balancing [21].

4. Proposed Scheme

In the proposed scheme Selfish Misbehavior Detection Algorithm has been introduced, the algorithm is implemented in various steps that include Channel Allocation Process, Cross Checking process and Penalty scheme.

Selfish Misbehavior Detection (SMD) Algorithm

The Selfish Misbehavior Detection (SMD) algorithm is depicted in Fig.1. The algorithm steps are follows,

Step 1: The Node enters the network.
Step 2: Cluster is formed and Cluster Head (CH) is allotted.
Step 3: Node requests the channel by sending Channel Request (CR) to the CH.
Step 4: Based on first come first serve basis, the CH allocates the channel to each node and sends Channel Allocation Message (CAM) to the nodes along with the time slots of all the nodes.
Step 5: If a node utilizes the channel more than the time slot allotted, then other nodes will send Report Message (RM) to the CH.
Step 6: The CH will do crosschecking process and if it confirms a selfish node then it sends Alert message to all nodes in the cluster.
Step 7: Once an alert is received, penalty scheme is applied to that particular selfish node.

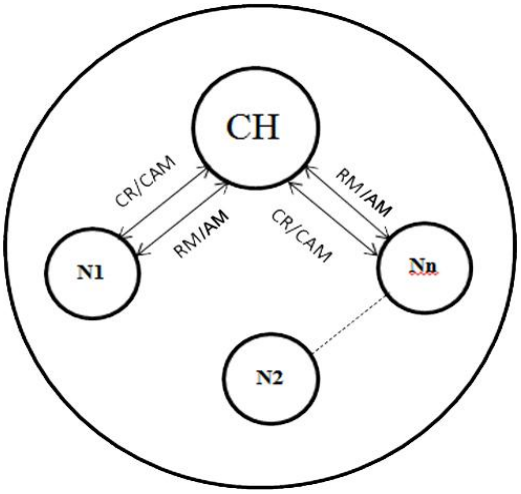
5. Channel Allocation Process

The MANET network is classified into n number of equal sized clusters. Every cluster will have a Cluster Head, which is responsible for channel allocation. Every node once enters the network will send Channel Request (CR) to the CH.

The cluster head will send a Channel Allocation Message (CAM) indicating the time slot for each node. The channel allocation will be done in first come first basis. Based on the time slot given, the nodes will utilize the channel without any collision. Every node knows the time slot of all other nodes in the network. So if any node misbehaves i.e. if any node uses the channel for long time span then other nodes identify that node as selfish node. If a node identifies a particular node as

selfish node, then it sends a Report Message (RM) stating that node as selfish node to the CH.

There is also a possibility for another attack behavior. That is, the selfish node may itself report some other node or normal node as selfish node to the CH. So the CH needs to crosscheck the report message received from any node within the cluster.



CR – Channel Request, CAM – Channel Allocation Message, RM – Report Message, AM – Alert Message

Fig. 1. MANET SMD Algorithm

6. Crosschecking Process

The crosschecking process is explained as follows: In every detection scheme, always there is a possibility for false positive and false negative. In case of false positive the normal node is reported as attacker/ selfish node whereas in case of false negative the attacker /selfish node is not reported as attacker node. This is serious concern that needs to be handled. In order to overcome this, crosschecking process has been introduced.

The CH will send a hello message to the node about which the report message is received. And will monitor that node. If the cluster head didn't get the reply message within the particular time span, then it will accept the Report Message and conclude that node as selfish node. But, if it gets the reply message within the time span, then there is a possibility that the node which sends the RM may be selfish node.

In order to confirm that, the CH will also send a hello message to the node, which have sent the report message (RM). If the CH didn't receive the reply message within the particular time span then the CH will conclude that, the node which sends that report message as selfish node. Else if, it receives the reply message within the time span then there is an issue that the node which sends the report message is selfish and the node which is reported as selfish might not be selfish node. In this case, the CH will wait for next report message (RM) about that particular node. If it receives the RM again then crosschecking phase will starts again. Else if it gets the CR from the same node then it will allocate the times slots with longer waiting time.

7. Penalty Scheme

The penalty scheme is not only implemented in data link layer but also in other higher layers. If a node is identified as selfish node, then the network layer will use the information about that particular node for routing. The network layer will refuse to forward the packets that are originating from the misbehaving node. If the CH confirms a node as a selfish node it sends the alert message (AM) to all other nodes in the cluster. Once an alert message is received then the nodes will add that node as selfish node in their blacklist. The nodes will stop communicating with the node in the blacklist, i.e. the nodes will not send or receive any data to or from the node in the blacklist.

The penalty scheme can be applied both temporally and permanently. In temporary penalty scheme the node will be isolated temporally, i.e. in case of waiting for next report message about the same blacklisted node. But if the CH confirms a node as attacker then permanent isolation will be applied.

8. Results

The SMD Algorithm has been implemented in NS2. The Throughput and Channel Occupation Duration of each node has been calculated and graph has been plotted with GNU Plot. Fig.3 illustrates the throughput without selfish node, so the graph is normal without fluctuations.

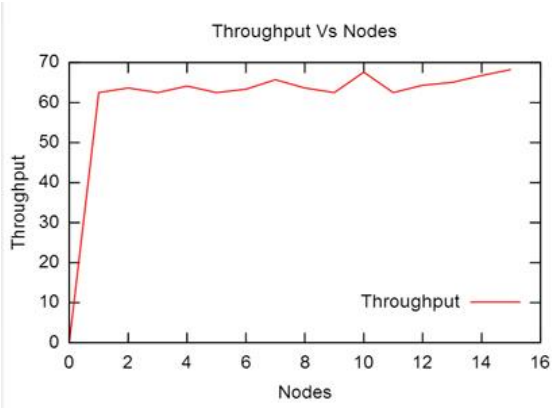


Fig. 3 Throughput vs. Nodes

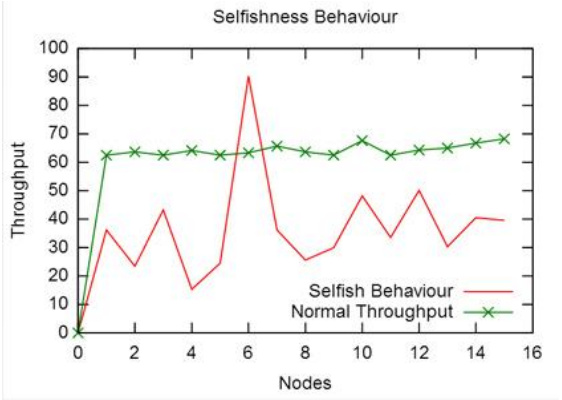


Fig. 4 Selfish Behavior

Fig.4 illustrates the comparison of throughput in the presence of selfish node and without selfish node. The throughput of the sixth node is very high i.e. abnormal compared to other nodes.

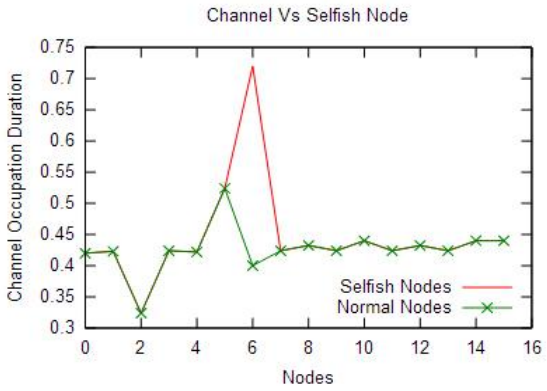


Fig. 5 Channel Occupation vs. Nodes

Fig.5. represents the comparison of Channel Occupation Duration of Selfish nodes and Normal nodes. Node sixth Channel Occupation Duration is very high compared to other nodes. These factors show that node six is the selfish node. Once the node is identified as selfish node then crosschecking process and penalty scheme will be applied on that node such that the node will be isolated from the cluster.

9. Conclusion

The proposed algorithm SMD detects selfish misbehavior effectively. After detection the selfish behavior node has been punished temporarily or permanently based on the scenario. The proposed algorithm also eliminates the probability of false positives and false negatives. In future work, the algorithm can be extended by sending the alert message to the neighbor cluster head in order to prevent from the selfish nodes.

References

1. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun*., vol. 18, no. 3, pp. 535-547, Mar. 2000.
2. A. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE J. Sel. Areas Commun*., vol. 25, no. 6, pp.1124-1134, Aug. 2007.
3. S. Radosavac, J. S. Baras, and I. Koutsopoulos, "A framework for mac protocol misbehavior detection in wireless networks," in 4th ACM workshop on Wireless security, Cologne, Germany, 2005, pp. 33–42.
4. H. Zhai, X. Chen and Y. Fang, "How well can the IEEE 802.11 wireless LAN support quality of service?" *IEEE Trans. Wireless Commun*., vol. 4, no. 6, pp. 3084-3094, Nov. 2005.
5. R. Ramaswami and K. Parhi, "Distributed scheduling of broadcasts in a radio network," in Proc. 8th Annu. Joint Conf. IEEE Comput.Commun. Soc. Technol. Emerging Converging, Apr. 1989, vol. 2, pp. 497–504.
6. Y. Cheng, X. Ling, W. Song, L. Cai, W. Zhuang, and X. Shen, "A crosslayer approach for WLAN voice capacity planning," *IEEE J. Sel. Areas Commun*., vol. 25, no. 4, pp. 678-688, May 2007.
7. A. A. C´ardenas, J. S. Baras, and K. Seamon, "A framework for the evaluation of intrusion detection systems," in *Proceedings of the 2006, IEEE Symposium on Security and Privacy*, Oakland, California, May 2006.
8. The MAdWiFi Driver, [Online.] Available: http://www.madwifi.org/.
9. Y. Rong, S. Lee and H. Choi, "Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis," in *Proc. IEEE INFOCOM*, 2006, pp. 1–13.
10. A. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE J. Sel. Areas Commun*., vol. 25, no. 6, pp. 1124-1134, Aug. 2007.
11. A. A. C´ardenas, S. Radosavac, and J. S. Baras, "Evaluation of detection algorithms for mac layer misbehavior: theory and experiments," *IEEE/ACM Trans. Netw.,* vol. 17, no. 2, pp. 605–617, 2009.
12. P. Kyasanur and N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *Proc. IEEE DSN*, 2003, pp. 173–182.
13. J. So and N. H. Vaidya, "Multi-channel MAC for ad hoc networks: Handling multi-channel hidden terminals using a single transceiver," in Proc. 5th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2004, pp. 222–233.
14. P. Kyasanur and N. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. Mobile Comput*., vol. 4, no. 5, pp. 502-516, 2005.
15. M. Cagalj, S. Ganeriwal, I. Aad and J. Hubaux, "On cheating in CSMA/CA Ad Hoc networks," Tech. Rep. LCA-REPORT-2004-017,2004.
16. J. Konorski, "Multiple access in Ad-Hoc wireless LANs with noncooperative stations," in *Proc. 2nd International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; and Mobile and Wireless Communications (NETWORKING)*, 2002.
17. Jin Tang, Yu Cheng and Weihua Zhuang, "An Analytical Approach to Real-Time Misbehavior Detection in IEEE 802.11 Based Wireless Networks", *IEEE INFOCOM 2011*.
18. Bora Karaoglu, Wendi Heinzelman, "A Dynamic Channel Allocation Scheme Using Spectrum Sensing for Mobile Ad Hoc Networks", IEEE Ad hoc and Sensor Networking Symposium, Dec-2012.
19. Jaiswal Amee V, Patel Mitesh R2 and Isamaliya Kajal K, "Dynamic Channel Allocation in Mobile Ad Hoc Network", www.ijaresm.net ISSN: 2394-1766
20. Bora Karaoglu, Wendi Heinzelman," Cooperative Load Balancing and Dynamic Channel Allocation for Cluster-Based Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 5, MAY 2015
21. Ming Li, Sergio Salinas, Pan Li, Jinyuan Sun, and Xiaoxia Huang, "MAC-Layer Selfish Misbehavior in IEEE 802.11Ad Hoc Networks: Detection and Defense" IEEE Transactions on Mobile Computing, Vol. 14, No. 6, June 2015

