IJETST- Volume||01||Issue||03||Pages 411-416||May||ISSN 2348-9480 2014

Open access Journal International journal of Emerging Trends in Science and Technology

A Survey on Acknowledgement Based Detection Schemes for Detecting Selfish Nodes in MANETs

Authors

Geetha D N[1], Roopa Banakar[2]

[1]Masters in Technology at Sapthagiri College of Engineering
Bangalore, India
Email:*geetha.dn@gmail.com*
[2] Assitant Professor, Department of Computer Science and Engineering
Sapthagiri College of Engineering, Bangalore, India
Corresponding Author

Geetha D N

Masters in Technology at Sapthagiri College of Engineering
Bangalore, India
Email:*geetha.dn@gmail.com*

Abstract:
Mobile Ad hoc Networks (MANETs) are very popular because of their widespread usage. In MANET, each node has to co-operate with each other to perform functions in the network. However some nodes do not participate in routing and forwarding packets which are not destined to them, in order to save their energy. Such misbehaving nodes which try to get benefitted from other nodes but refusing to forward other nodes packets can severely degrade the performance of the whole network. In MANETs, detection of such misbehaving nodes is very important. In this survey, a detailed study of misbehaving nodes, their characteristics and their effects in various layers of the network are discussed. Moreover, various detection schemes which deal with misbehaving nodes are also considered in the discussion. This paper discusses the different acknowledgement schemes for misbehaving node detection in MANETs.
Keywords— Mobile Ad hoc Networks, Selfishness, Pathrater

1. Introduction

Mobile Ad hoc NETwork (MANET) is self configuring network of mobile node connected by wireless links and considered as network without infrastructure. Nodes can communicate directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of routing protocols [1]. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, non-cooperation may occur which can severely degrade the performance of network.

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already enter the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defense line of network become

ineffective. Since internal attacks are performed by malicious nodes which behave well before they are compromised, therefore it becomes very difficult to detect such attacks [1].

Node's misbehavior can be classified as malfunctioning, selfish or malicious nodes [2][3]. Malfunctioning nodes suffer from hardware failures or software errors. Selfish nodes refuse to forward or drop data packet. It can take participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources. Malicious nodes use their resource and aims to weaken other nodes or whole network by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control.

2. Misbehaving Nodes in MANETS

Node misbehavior can be defined as any form of disobeying the protocol specification to obtain the given goal at the expense of honest participants. A node may misbehave in order to save their resources (process time and energy). A misbehaving node continues to perform any type of misbehavior till it gain sufficient benefits. Fig. 1 shows the packet forwarding in a network with regular nodes and in the presence of misbehaving nodes.

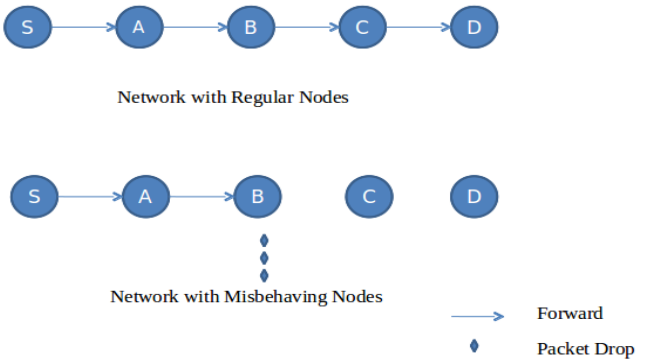

Fig. 1 Network with regular nodes Vs misbehaving nodes

Misbehaving nodes can be usually classified as selfish nodes and malicious nodes [4]. Selfish nodes are those nodes which misbehave to save their energy or power whereas malicious nodes disturb the network operations by its malicious activities. These nodes may participate in the route discovery and route maintenance phases and transmit control packets which can benefit itself [5]. However they refuse to forward data packets. Malicious nodes, on the other hand, will participate actively in both route discovery and maintenance phases and transmit the control packets since they need a path to send the data packets so that they can alter or drop those packets.

3. Network Layer Misbehavior

In MANETs, packet forwarding requires the cooperation of the intermediate nodes since the packets send from a source node has to be relayed via the intermediate node to the destination [6]. In Ad hoc networks, there are no dedicated nodes which are responsible for forwarding and routing. Hence each node expects the following services from its neighbors:

- Routing service: This requires nodes to create route table by the exchange of Route Request Packets (RREQ).
- Forwarding service: Based on the destination IP address, forwards the packets to the next hop on its path to the destination by referring the route table.

In the Ad hoc scenario, following are the possible violations in network layer:

1) Nodes participate in routing process but not in data forwarding process: Misbehaving nodes behave well in the route discovery phase and route maintenance phase but refuse to forward the data packets [7]. In MANETs, RREQ packet size is small. Any node can sacrifice the power for forwarding the packets. But data packets are very large packets. So, misbehaving nodes mainly drop data packets rather than control packets [8].

- Individual dropping: Nodes may drop all or certain percentage of data packets
- Colluded dropping [9]: Two misbehaving nodes collude in the network such that the misbehavior of one node will not be reported by the other node.

2) Nodes that does not participate in routing: Some misbehaving nodes do not forward control packets itself [10]. In MANETs, the node is not ready to participate in the forwarding process even for small size packets or in critical state. The transmission path will not be established and hence these nodes need not participate in the data transmission.

3) DoS Attack [11]: Malicious nodes generate false messages in order to disrupt the network's operation or to consume other nodes' resources.

4. Network Layer Based Detection Schemes

Network layer based detection schemes are categorized into following:

4.1 Credit Based Scheme

In this scheme, credit/incentives are provided to the nodes performing network operations. Widely acclaimed credit based schemes are Packet Purse Model (PPM) and Packet Trade Model (PTM). These schemes may need extra protection for payment system.

4.2 Reputation Based Scheme

In this scheme, nodes collectively co-operatively detect and declare misbehavior of nodes in the network. Such a declaration is carried out throughout the network and misbehaving node is removed from the network. 'Confidant Protocol' is an example of reputation based scheme.

4.3 Acknowledgement Based Scheme

In this scheme, acknowledgements are sent by the receiver to sender about the successful reception of data packets. There are several acknowledgement based schemes proposed for misbehavior detection such as 1-ACK, 2-ACK, SACK, TWO-ACK, N-ACK etc. Acknowledgement schemes proposed have been discussed in next sections of this paper.

5. Acknowledgement Based Schemes

5.1 Watch Dog and Path Rater

This scheme in [10], which is a passive acknowledgement based scheme, considers the problem of misbehaving nodes who agree to forward the packets but fail to do so. Watchdog scheme makes use of overhearing mechanism to monitor the neighboring nodes whether they have forwarded the packets or not. Path rater finds out the best route by avoiding the misbehaving nodes in the path. Since this scheme uses an alternate path for further packet forwarding, the misbehaving nodes in the path stay as such, not being isolated. So it continues to utilize the network services. This scheme fails to work properly in the presence of ambiguous collision, receiver collisions, limited transmission power and false misbehavior report.

5.2 TWOACK

Balakrishnan et al. proposed a scheme TWOACK in [12] to solve the problem of the receiver collisions and limited transmission power. This scheme was implemented as an add on to the existing DSR protocol. Suppose node A has discovered a route to node F with a source route A->B->C->D->E->F. In this scheme, when node B forwards a packet send from A towards C, after reception of the packet at C, it is required to send an acknowledgement back to A, which is two hops away from C. This acknowledgement coming from C indicates that B has forwarded the packet send from A. Same procedure is carried out by all the network nodes along the source route. If A did not receive an acknowledgement from C, it suspects B as misbehaving node. TWOACK scheme contributes for traffic congestion in the network since it is expecting an acknowledgement for each and every packet that is transmitted.

5.3 S-TWOACK

S-TWOACK (Selective TWOACK) scheme reduces this congestion problem by sending a single acknowledgement for a number of packets instead of a single packet. This scheme also adds overhead to the routing protocol because of the multiple acknowledgements for each packet along the path. The drawback of TWOACK scheme is that it provides no authentication for the acknowledgement packet which has been sent form the receiver and it also increases the routing overhead.

5.4 Enhanced TWOACK Scheme

An extension to the 2ACK scheme proposed by A Al-Roubaiey et al. is also a network layer acknowledgement-based scheme. In the previous scheme, it could detect only misbehaving links instead of exact misbehaving nodes. This paper [13] proposes a solution to find out the exact misbehaving node in the links when we have a destination node in the other end.

Here, the source node will wait for an acknowledgement from destination after the successful reception of the packet at the destination. If an acknowledgement did not reach the source within a specific timeout, then it should switch to TWO-ACK mode. In the detection and response module of this scheme, a node which discovers another node as malicious, will inform the source node by sending an alarm. An alarm is a small packet which is generated by the routing

protocol. It will carry the malicious node id. Each node in the path will forward the alarm and learn from it about the malicious node.

5.5 AODV+ACK+PFC

Mamatha et al. [14] investigated the performance degradation caused by such malicious nodes (misbehaving) in MANETS. They have proposed and evaluated a technique called, (AODV+ACK+PFC) to detect and mitigate the effect of such routing misbehavior. In future the enhancement may be done by evaluating for more number of nodes and network parameters. Further the scheme may also be extended for identifying and preventing more number of network layer attacks; so that the approach can be made more robust against attacks.

5.5 CBC-X

Rajaram et al. [15] proposed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, they have designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the Cipher Block Chaining (CBC-X) mode of authentication and encryption.

5.6 Detecting misbehaving nodes by Improved ACK scheme

Anandukey et al. [1] investigated the misbehavior of nodes and a new approach is proposed for detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol such as DSR and is based on sending acknowledgement packets for reception of data packets and using promiscuous mode for counting the number of data packets such that it overcomes the problem of misbehaving nodes. Also proposed approach has lesser routing overhead and more advantageous because it requires lesser number of acknowledgment packet transmission. In future they will include some authentication mechanism to make sure that the ACK packets are geniune and also including mechanism to punish misbehaving nodes.

5.7 Timer Based Acknowledgement Scheme

This Scheme detects and isolates the misbehaving nodes and also finds alternate case in case number of misbehaving nodes in the route is greater than the minimum count. This scheme maintains good packet delivery ratio with reduced packet drop, delay and overhead compared to secure on-demand routing protocol. In this scheme, the groups of nodes on the route are divided into sets. Assuming 2 sets, the source node of the 1 st set must get an acknowledgement from destination node after successful reception of data packet. Also the destination node of 2 nd set must send the acknowledgment to the source node of 1 st set. In order to avoid delay and overhead problems, this scheme proposes detection timer. Detection timer has specific time interval assigned to it. On forwarding the packet, source node starts the detection timer.

A forward counter is maintained which is updated during the packet entering and leaving the node. When the detection timer expires, the destination node is checked for those data packets which have received and forwarded by the node. If the forward count is below threshold, negative acknowledgement (NACK) is sent to the source node of first set. Otherwise the positive acknowledgement (PACK) is sent. This process is repeated for each group of nodes. The advantage of this scheme is that acknowledgement is not sent for reception of each data packet since it is processed in groups and it minimizes the waiting time for acknowledgement and also overhead reduces. Using pathrater alternative route can be chosen by rating the nodes.

6. Comparison

Table 1: Comparison of Acknowledgement Schemes

Scheme Name	Detects misbehaving node/Link	Remarks
Watchdog and Pathrater	Node	fails to work properly in the presence of ambiguous collision, receiver collisions, limited transmission power and false misbehavior report.
TWOACK	Link	Reliability of network decreases on increase in number of node in route
S-TWOACK	Link	Can cause false-alarms due to loss of genuine TWOACK packets.
Enhanced TWOACK	Node	Detects the exact misbehaving node in the link.
Improved ACK Scheme	Node	Sending of acknowledgement packets and counting the number of data packets individually is time consuming and even causes overhead.
Timer Based Acknowledgement Scheme	Node	Finds alternative route and reduces packet drop, delay and overhead compared to other schemes

7. Conclusion

MANETs are highly dependent on the cooperation of all of its members to perform networking function. This makes it highly vulnerable to misbehaving nodes. In the presence of misbehaving nodes the performance of the network is degraded severely. Acknowledgement based schemes mentioned in this paper detects and prevents the misbehavior in the MANET. Although the acknowledgement schemes add an overhead to the network, these help in increasing reliability and network throughput. Tradeoff needs to be considered between routing overhead and network parameters like reliability and throughput while selecting the scheme for implementation.

The timer based acknowledgement scheme attains good packet delivery ratio with reduced packet drop, delay and overhead, when compared with existing acknowledgement based scheme. Pathrater can be used to find an alternative route in case of more number of misbehaving nodes is detected in the route.

References

1) S. Anandukey and M. Chawla, “Detection of packet dropping attack using improved acknowledgement based scheme in MANET,” International Journal of Computer Science Issues I, vol. 7, no. 1, pp. 12-17, 2010.
2) S. Dhanalakshmi and M. Rajaram, “A reliable and secure framework for detection and isolation of malicious nodes in MANET,” International Journal of Computer Science and Network Security, vol..8, no.10, pp. 184-190, 2008.
3) M.I.M. Saad and Z. A. Zukarnain, “Performance analysis of random-based mobility models in MANET routing protocol, “ European Journal of Scientific Reasearch, vol. 32, no. 4, pp. 444-454, 2009.
4) Sangheethaa Sukumaran, Venkatesh.J, Arunkorath, “A Survey of Methods to mitigate Selfishness in Mobile Adhoc Networks”, in International Journal of Information and Communication Technology Research, Volume 1 No. 2, June 2011.
5) Younghwan Yoo and Dharma P. Agrawal, “Why Does It Pay To Be Selfish In a MANET?”, in IEEE Wireless Communications, December 2006.

6) Mangesh, Pradeep, Ali, "Countermeasures of Network Layer Attacks in MANETs", in IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.
7) Shailender Gupta, C. K. Nagpal and Charu Singla, "Impact Of Selfish Node Concentration In MANETS", in International Journal of Wireless & Mobile Networks (IJWMN), Vol. 3, No. 2, April 2011.
8) Li Zhao, Jose, "MARS: Misbehavior Detection in Ad Hoc Networks", in IEEE GLOBECOM, 2007.
9) Graffi, Parag, Matthias, Steinmetz, "Detection of Colluding Misbehaving Nodes in Mobile Ad hoc and Wireless Mesh Networks", in IEEE Global Communications Conference, November 2007.
10) Marti, Giuli, Lai, Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in Proceedings of ACM, 2000.
11) Mieso K. Denko, " Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", in SYSTEMICS, CYBERNETICS AND INFORMATICS, Vol. 3, No. 4, 2003.
12) Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", in IEEE Transactions on Mobile Computing, May 2007, 536-550.
13) Roubaiey, Sheltami, Mahmoud, Shakshuki, Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", in proceedings of IEEE International Conference on Advanced Information Networking and Applications, PP. 634-640, 2010.
14) G. S. Mamatha and S. C. Sharma, "A new combination approach to secure manets against attacks," International Journal of Wireless & Mobile Networks, vol. 2, no. 4, pp. 71-80, 2010.
15) Rajaram and S. Palaniswami, "Malicious node detection system for mobile ad hoc networks," International Journal of Computer Science and Information Technologies, vol. 1, no. 2, pp. 77-85, 2010.