SURVEY ON ACKNOWLEDGEMENT BASED SCHEMES FOR MISBEHAVIOR DETECTION IN MANET

[1]MRUNAL PATHAK, [2]JYOTI HOTTE

[1]Information Technology Department, AISSMS IoIT, Pune University, India
[2]Computer Engineering Department, GHRCEM College, Pune University, India
Email: hemangikulkarni21@gmail.com, hotte.jyoti@gmail.com

Abstract— MANET (Mobile ad hoc network) is a collection of mobile nodes which communicate with each other directly or via other nodes which works as router. Nodes in MANET can move independently in any direction so the topology changes rapidly and unpredictably over time.
Routing protocols of MANETs are designed considering that all participating nodes collaborate and communicate in harmony. However, participating nodes need energy and other resources to perform network functions, which can lead to misbehavior of node. Misbehaving nodes degrades network performance. Several acknowledgement based schemes have been proposed to detect misbehaving nodes in MANET. This paper aims at providing the survey and comparison of various acknowledgement schemes which have been proposed to detect misbehavior in MANET.

Keywords—MANET, Misbehaving Nodes, Ad Hoc Networks, ACK**.**

I. INTRODUCTION

MANET is infrastructure less network having a group of mobile nodes which interact with each other for data transmission. Nodes move freely and independently in any direction changing the topology rapidly and unpredictably. Each node forwards traffic unrelated to its own use and therefore be a router. Routing protocols for MANET are based on the assumption that all participating nodes are fully cooperative. But, due to the open structure node misbehavior may exist. In MANETs, routing misbehavior degrades the performance. Specifically, nodes participate in the route discovery and maintenance processes but refuse to forward data packets. MANET suffers from a great efficiency loss due to the misbehaving nodes which may constrained by the resources such as battery power and bandwidth. Different approaches have been already proposed to detect and prevent the misbehavior in MANET. Different acknowledgement schemes which have been proposed are described in following sections of the paper.
This paper is organized in 5 sections. Misbehavior Detection in MANET is discussed in Section 2; in section 3 various acknowledgement schemes are discussed; comparison of described acknowledgement schemes is covered in section 4; conclusion is proposed in section 5.

II. MISBEHAVIOR DETECTION IN MANET

Routing protocols performs two important functions:
1. Routing function
2. Data-Forwarding function
Routing function is involved in route discovery and route maintenance activity whereas Data-Forwarding function is involved in forwarding data packets towards the destination through already established route. To perform these functions, trusted working environments are needed which may not be available always and in such a situation network will be vulnerable to various attacks launched by misbehaving nodes. Both routing and data forwarding function can be affected with the presence of misbehaving nodes. Misbehaving nodes can cause different types of attacks like packet eavesdropping, message tampering, black whole attack, gray whole attacks, etc. So primary challenge in MANET is to detect misbehavior and mitigate same. Misbehaving node dropping all packets is shown as follows:

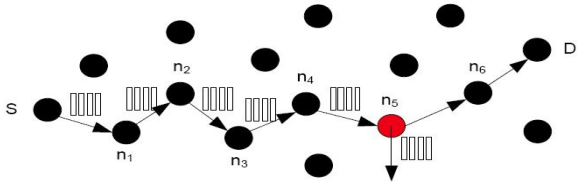

Fig 1: Misbehaving Node

In the Fig above, node n5 is misbehaving node as it drops the packets received and does not forward to other nodes in the path. Different schemes proposed to avoid nodes misbehavior in MANET can be classified as:

A. 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.

B. 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. 'Watchdog & Pathrater' and 'Confidant Protocol' are examples of reputation based scheme.

C. Acknowledgement Schemes

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.

III. ACKNOWLEDGEMENT BASED SCHEMES

In this scheme, acknowledgements are sent by end receiver to inform the sender about successful reception of data packets up to some locations of continuous data stream. All acknowledgement based schemes, adds to routing overhead in the network but increases reliability and throughput of the network. Existing acknowledgement schemes and their behaviors are described below:

D. 1- ACK Scheme

This scheme is based on single or 1-hop acknowledgement packet that is sent by receiver to sender. ACK scheme is an end-to-end acknowledgement scheme in which source node sends out an ACK data packet to the destination node. If all the nodes on the route between source and destination are co-operative, data packet is received successfully by destination and then it sends back an ACK acknowledgement packet along the same route but in reverse order.

In this scheme, when node forwards data packet to the next node in the routing path, the receiving node will send back the acknowledgement called ACK which indicates that data packet has been received successfully.

This scheme overcomes problems such as overhearing, ambiguous collisions, receiver collisions, and limited transmission powers but increases routing overhead to large extent.

E. SACK (Selective Acknowledgement) Scheme

This is an enhancement to an end-to-end acknowledgement scheme ACK proposed in. This scheme is applied to detect misbehaving node instead of misbehaving link.

This scheme improves performance over ACK scheme by reducing routing overhead and by increasing detection efficiency by applying node detection.

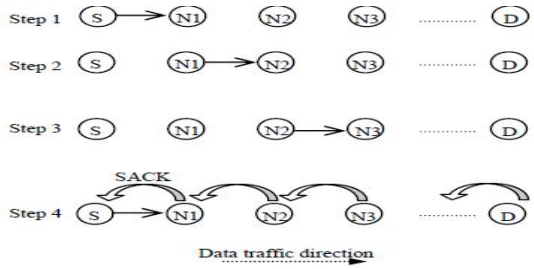

Fig 2: S-ACK Scheme

In this scheme, acknowldgement packet will not be sent for every received packet. Single SACK packet will be sent for certain amount of data packets received from same source node. Thus is reduces routing overhead substantially.

F. TWOACK scheme

TWOACK scheme proposed by Liu et al detects misbehaving link by acknowledging every data packet transmitted over each 3 consecutive nodes along path from source to destination. In this scheme, packet TWOACK is sent back 2 hops for every data packet received. This increases reliability as well as network overhead.

In this scheme, if the source does not receive a TWOACK acknowledgement packet for data packet sent, the next hop's forwarding link is claimed to be misbehaving.

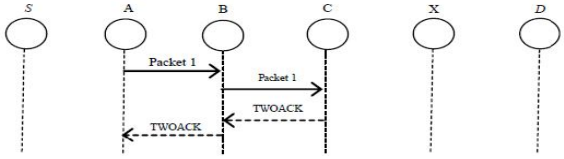

Fig 2 : TWOACK Scheme

Suffer from problem that, it fails to detect malicious nodes in the presence of false misbehavior report and forged ACK packets. In this scheme source node immediately trusts the misbehavior report provided by other nodes.

In a network where up to 40% of the nodes are misbehaving, the TWOACK scheme improved the end to-end packet delivery ratio from around 70% to almost 90% while increasing the overhead from 4% to 7%.

G. Selective TWOACK (S-TWOACK) Scheme

This scheme is derivative of TWOACK scheme in which the TWOACK packet acknowledges the receipt of number of data packets and not only one data packet. This scheme reduces the network overhead compared to TWOACK Scheme.

The S-TWOACK scheme which is a based on TWOACK scheme only, achieves almost same performance improvement without any routing overhead but with some expected increase of false alarms.

H. AACK (Adaptive Acknowledgement) Scheme

Sheltami et al. Proposed a new scheme which is based on TWOACK scheme. It is a combination of TWOACK and end-to-end acknowledgement scheme ACK. As compared to TWOACK, this method significantly reduces network overhead and still maintains same network throughput.

Suffer from problem that, it fails to detect malicious nodes in the presence of false misbehavior report and forged ack packets.

I. EAACK (Enhanced Adaptive Acknowledgement) Scheme

Scheme EAACK, tackles problems such as false misbehavior, limited transmission power and receiver collision. EAACK consists of 3 parts: acknowledgement ACK, Secure-Acknowledgement S-ACK and Misbehavior Report Authentication MRA. This scheme is capable of detecting malicious nodes even in case of false misbehavior report.

In this scheme source node does not trust misbehavior report without confirming the misbehavior of nodes. During MRA mode, source node seeks for alternate routes to destination using DSR routing. Alternate route is used to confirm misbehaving report. If the destination receives MRA packet, it is concluded that the report is false and whoever has generated that report is marked as malicious else it is concluded that misbehavior report is trusted. In order to ensure the integrity, all the acknowledgement packets in this scheme are digitally signed by nodes.

J. 2-ACK Scheme

2-ACK is network layer scheme to find misbehaving links and to mitigate their effects. In this scheme, receiver node sends 2ACK packets to a fixed route of 2 hops (3 nodes) in the opposite direction of data traffic route as mentioned in the fig below.

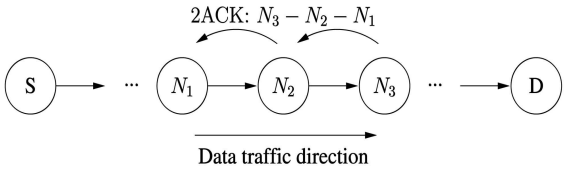

Fig. 3: 2-ACK Scheme

Because of acknowledging only selected received data packets gives the 2ACK scheme better performance respect to the routing overhead. S-TWOACK and 2-ACK are also different in a way that, S-TWOACK acknowledges receipt of number of data packets where as 2-ACK acknowledges only one data packet.

This technique overcomes weaknesses of the Watchdog/path rater like ambiguous collisions, receiver collision and power control transmission.

Advantages of this scheme over watchdog:

1. Reliable data transmission
2. Reliable route discovery
3. Limited transmission power
4. Limited overhearing range

K. Random 2-ACK Scheme

This scheme is based on simple 2-hop acknowledgement that is sent by the receiver of the next-hop link. In order to detect misbehavior, sender maintains a list of IDs of data packets that have been sent out but have not been acknowledged. The ID created will stay on the list till the reception of 2-Ack packet or timeout. Two counters are maintained. Counter for packets received Cpkt and counter for missed acknowledgement Cmis. If the 2-Ack is received after timeout, the count of missed acknowledgements is incremented. If the ratio of missing 2Ack packets Cmis/Cpkt is greater than threshold ratio, then the link is declared as misbehaving.

This scheme is similar to 2-ACK scheme except that, only fraction of data packets are acknowledged randomly in random 2-ack scheme. Such a fraction is called as Acknowledgement ratio Rack. The overhead of 2Ack packet transmission can be tuned by changing Rack dynamically.

L. N-ACK Scheme

N-ACK is an extension to the 2-ACK Scheme. This scheme uses multi-hop acknowledgement in order to detect and isolate misbehaving nodes.

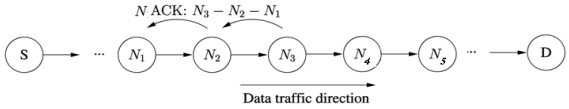

Fig. 4: N-ACK Scheme

It defines N-ACK packet which has fixed route of N number of hops in the direction opposite to the original data traffic. On receiving data packet, destination sends back NACK packet. Each node has to maintain a list of data packets sent and list of data packets forwarded. Data packet and NACK packet keep the track of route they travel which are compared by source node. In case the paths are same, source node concludes that there are no misbehaving nodes exist in the path. In case 2 paths vary, node in source to destination path from where path varies in destination to source path is detected as misbehaving node and is isolated.

M. 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 1st set must get an acknowledgement from destination node after successful reception of data packet. Also the destination node of 2nd set must send the acknowledgment to the source node of 1st 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 period for acknowledgement and also overhead is reduced.

IV. COMPARISON

Table 1: Comparison of ACK Schemes

Scheme Name	'N'-hop ACK	Detects misbehaving node/link	Highlights
1-ACK	1	Node	1. Avoids Watchdog problems like Over hearing, ambiguous collisions, receiver collisions and limited transmission power 2. Higher routing overhead than SACK
SACK (Selective Acknowledgement)	1	Node	1. Less overhead than 1-ACK 2. ACK is sent for selective packets
TWOACK	2	Link	1. More reliable than 1-ACK and SACK 2. Reliability of network decreases on increase in no of nodes in route
S-TWOACK (Selective - TWOACK)	2	Link	1. Derivative of TWOACK Scheme 2. Less overhead than TWOACK 3. Can cause false-alarms due to loss of genuine TWOACK packets
AACK (Adaptive Acknowledgement)	2	Link + node	1. Based on TWOACK Acknowledgement 2. Less overhead than TWOACK 3. Cannot detect malicious nodes in presence of false misbehavior report and forged ACK packets
EAACK (Enhanced Adaptive Acknowledgement)	2	Node	1. Enhanced security by using digital signature 2. Uses S-ACK (secure ACK)
2-ACK	2	Link	1. Acknowledges receipt of only one data packet 2. More reliable than earlier schemes like watchdog, 1-Ack, TWOACK
Random 2-ACK	2	Link	1. Extension of 2-Ack scheme 2. Less overhead than 2-Ack because of random acknowledgements
N-ACK	N (N= no. of nodes)	Node	1. Highly reliable 2. Very high network overhead 3. Uses both ACK and NACK
Timer Based Acknowledgement	X (X= no of nodes in set)	Node	1. Along with detection and isolation of misbehaving node, finds alternate route 2. Reduces packet drop, delay and overhead compared to other schemes

CONCLUSION

MANETs are an area of active research due to their potentially widespread applications. 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.

REFERENCES

[1] Usha.Sakthivel and Radha.S,"Routing layer Node Misbehavior Detection in Mobile Ad hoc Networks using N-ack Schemes", International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012 Singapore.

[2] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment- Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, Vol-6 , Issue 5, May 2007, pp. 536-550.

[3] Ashish Kumar, Vidya Kadam, Subodh Kumar and Shital Pawar,"An acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANETS", International Journal of Advances in Embedded Systems Volume 1, Issue 1, 2011.

[4] K. Balakrishnan, J. Deng, and P.K. Varshney,"TWOACK:Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless comm.and Networking Conf.,Mar.2005.

[5] U.Sharmila Begam, Dr. G. Murugaboopathy, "A RECENT SECURE INTRUSION DETECTION SYSTEM FOR MANETS", nternational Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013.

[6] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, ―Video transmission enhancement in presence of misbehaving nodes in MANETs, Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009..

[7] Prof. Shalini Wankhede,"2ACK-Scheme: Routing Misbehavior Detection in MANETs Using OLSR", International Journal of Advanced Research in Computer Engineering and Technology. Volume 1, Issue 5, July 2012

[8] Meghana J R, Manasa S., Muneshwara M.S., Anil G.N., " IMPLEMENTATION OF 1-ACK SCHEME FOR DETECTING MISBEHAVIOUR NODES IN MANET", International Conference on Computing and Control Engineering (ICCCE 2012), 12, 13 April, 2012

[9] Ramasamy Murugan, Arumugam Shanmugam, "A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET", International Journal of Network Security, Vol.15, No.4, PP.241-247, July 2013

[10] Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G., Harish Redd, " A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks"

[11] S. Marti, T. Giuli, K. Lai, and M. Baker,"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. MobiCom, Aug. 2000.

[12] Jin-Shyan Lee, "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008.

[13] G.Muruga Boopathi, N.Insozhan, S.Vinod, "Selfish Nodes Detection Using Random 2ack In MANET s", IJESE ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[14] Y. Zhang, W. Lee and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM MONET Journal 2003

[15] Nimitr Suanmali, Kamalrulnizam Abu Bakar and Suardinata, "Selective Acknowledgement Scheme to Mitigate Routing Misbehavior in Mobile Ad Hoc Network", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.

[16] L. Zhou and Z.J. Haas , "Securing Ad Hoc Networks", in IEEE Network Magazine,1999.Volume 13, Nov./Dec. 1999, Issue 6. Pages.551-567, Year of Publication: 2003 ISBN: 0-8493-1332-5