ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol3, Issue 5, May 2016

Misbehaving Node Detection using Secure Acknowledgement in MANET

[1] Chandini K.C, [2] Ganavi. N, [3] Meghana K.M,[4] Kalpana M.S, [5] G.Manjula, [6] Sowmya.A.M
[1] [2] [3] [4] [6] UG Scholars, [5] Asst Professor
Dept of Computer Science and Engineering, SSCE, Anekal, Bangalore

Abstract— **Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes. MANET is preferred in variety of applications such as military, disaster stuck areas, emergency recovery etc. MANET is vulnerable to various attacks due to its open medium and wide distribution of nodes. This itself emphasize the importance of security and need for an efficient system, for example intrusion detection system in MANET. The Misbehavior such as, delay or drop in data packets or acknowledgement packets, drop packets and modify routing information etc. are present. These Misbehavior need to be detected well in advance to keep network secure. In this paper we propose and implement, new IDS named as Secure Acknowledgement (ACK) System. The Secure ACK system is purely an acknowledgement based technique. The type of Misbehavior detected by proposed system is about delay in packet transmission. In this system, for every three consecutive nodes in the route, the third node is required to send back an acknowledgement packet to the first node in the group. Based on the non-receipt of ACK packet within predefine time to the first node in the group, it reports about Misbehavior activity in the network. As soon as the proposed system detects misbehaving node present in the network, it stops the further data transmission. So, the misbehaving node will not be able to damage network thereafter.**

Keywords— **MANET; Vulnerability in MANET; Intrusion Detection System; Acknowledgement Based Schemes; Misbehaving Nodes; Secure ACK.**

I. INTRODUCTION

Mobile Ad hoc Network termed as MANET is a collection of mobile nodes. Mobile nodes can be cell phones, PDAs, laptops etc. Every node in MANET has ability to transmit and receive data. Such mobile nodes in MANET can communicate with each other without fixed infrastructure. MANET can create its own self configuring and self maintaining network without centralized infrastructure. Basically there are two types of MANET: Close and Open [1] . In closed MANET, all mobile nodes cooperate with each other for common goal. On the other hand in open MANET different mobile nodes having different goals share resources and hence ensure global connectivity. MANET has two types of networks, one is

Single hop and another is Multi hop. There can be direct or indirect communication within nodes. In single hop network all nodes are within same range and can communicate directly which is known as direct communication. In multi hop network nodes rely on neighbors to communicate beyond transmission range which is known as indirect communication [2]. Communication in the network depends upon the trust on each other and communication works properly if all nodes co-operate with each other for data transmission.

Misbehavior of Nodes

In MANET, "Misbehavior" refers to node that does not behave in proper way. In other words, if behavior of node deviates from its specification or set of behaviors then the node is said to be misbehaving [3],[4]. Misbehavior takes place in different ways, such as, delay data packets or acknowledgement packets, don't forward packet to save own resources, drop data packets or acknowledgement packets, drop packets and modify routing information, forward control packets while dropping data packet types of Misbehavior namely, failed / malfunctioned, selfish and malicious [4].

x Failed / Malfunctioned: A node malfunctions because of hardware and software problems, climate, radio channel, link breakdown, accidental physical damage.

x Selfish: Selfish nodes have passive Misbehavior. Selfish nodes do not intend to directly damage other nodes and do not cooperate. It saves battery life for own communication. A selfish node is unwilling to spend CPU cycles and available network bandwidth to forward packets.

x Malicious: Malicious nodes have active Misbehavior. Malicious node intentionally damages network and interrupt operations. A malicious node may drop the packets, modify the routing information. It may not give priority to battery power saving.PROBLEM STATEMENT

In literature, there are various IDSs proposed to detect misbehaving node in the network, but each system has some limitations. Aim of the proposed IDS is to overcome those limitations and efficiently detect misbehaving node present in the network. Type of Misbehavior to be detected using proposed IDS is about Delay in transmission of Data packets or Acknowledgement packets. Proposed system is designed to overcome limitations of Watchdog and TWOACK Technique. Some drawbacks of watchdog system stated above are discussed in detail below.

II . RECEIVER COLLISION

As shown in Fig.1, there are six nodes with 'S' as source node, 'D' as destination node and N1, N2, N3, N4 are intermediate nodes in path. When, Node N1 sends Packet 1 to node N2, it tries to overhear if node N2 forwarded this packet 1 to node N3; meanwhile, node N4 is forwarding Packet 2 to node C. In such case, node N1 overhears that node N2 has successfully forwarded Packet 1 to node N3 but failed to detect that node N3 did not receive this packet due to a collision between Packet 1 and Packet 2 at node N3.

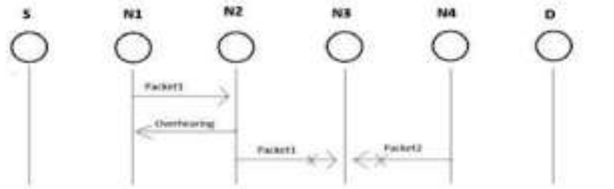

Fig.1 Receiver Collision

III. LIMITED TRANSMISSION POWER

As shown in Fig.2, there are six nodes with 'S' as source, 'D' as destination and N1, N2, N3, N4 as intermediate nodes. Packet 1 is getting transmitted from source node to destination node. During transmission in order to preserve its own battery resources, node N2 intentionally limits its transmission power. So, packet transmission is strong enough to be overheard by node N1 but too weak to be received by node N3.

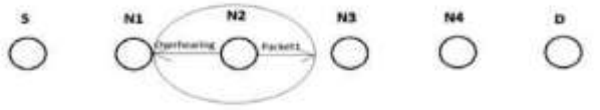

Fig.2 Limited Transmission Power

As shown in Fig.3, although node N1 successfully overheard that node N2 has forwarded packet 1 to node N3, node N1 still reported node N2 as misbehaving. Due to open medium and remote distribution of MANTEs, attackers can easily captures and compromise one or two nodes to achieve this false Misbehavior report attack.

IV. PROPOSED SYSTEM

A. Proposed Solution

In this paper we propose and implement, new IDS named Secure ACK. The system is proposed to overcome drawbacks of Watchdog and TWOACK stated before. Secure ACK system is purely an acknowledgement based technique. It is based on Enhanced Adaptive Acknowledgement (EAACK) system [12], but includes enhancement in a key technique for detection of misbehaving node present in network. The type of Misbehavior to be detected by proposed system is about packet delay or acknowledgement delay. It detects this malicious activity in the network within very less time and stops data transmission, so the misbehaving node will not be able to damage the network thereafter.

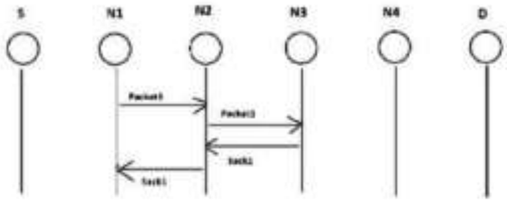

Fig.4 Secure ACK Mechanism

In EAACK system, if node N1 does not receive the SACK acknowledgement packet within a predefined time period, both nodes N2 and N3 were reported as malicious. Moreover, a Misbehavior report for node N2 and N3 will be generated by node N1 and sent to the source node. Using Misbehavior Report Authentication mechanism [12], the report about node N2 and N3 is verified. The verification was in terms of whether packets received at destination or not. If packet is received at destination through nodes N2 and N3, it concludes that report was false and node creating such report is malicious node. But again, it was not capable to detect which node intentionally delays data or acknowledgement packets.

In Secure ACK system, if node N1 does not receive the SACK acknowledgement packet within a predefined time

period, nodes N2 and N3 are reported as malicious by node N1. In such case our proposed system immediately checks for Per Hop Delay between nodes N1, N2 and N3 i.e. within group of three consecutive nodes. For nodes N1 and N2, if data packet is not received within predefined time period at node N2 then, node N1 is concluded as misbehaving.data packet is not received within predefined time period at node N2 then, node N1 is concluded as misbehaving.
Secure ACK Algorithm

Input: A network topology with n nodes.
Output: Detect misbehaving node in network of n nodes. Condition: Misbehavior is of type packet delay.

Step 1: Create network of n nodes.

Step 2: Set source node ‘S’ and destination node ‘D’.

Step 3: Use routing protocol to find path between given source and destination. Suppose path is, S -N1 - N2 - N3 - N4 - D.

Step 4: Allow data traffic to flow between source and Destination through specified path.

Step 5: For successive 3 consecutive nodes (for e.g. ‘S - N1 - N2’ or ‘N1- N2 - N3’ and so on), as soon as packet reaches third node in each group of 3 nodes, send SACK packet to first node in group through same route in reverse order.

Step 6: Calculate Intermediate Round trip time (IRTT) wherein no malicious node present in the network. Let’s consider group of 3 nodes as N1-N2-N3,

$$IRTT\ (N1, N2, N3) = TDatapkt\ (N1, N2) + TDatapkt\ (N2, N3) + TSACKpkt\ (N3, N2) + TSACKpkt\ (N2, N1) \qquad (1)$$

Where, TDatapkt is time required for Data Packet to travel from one node to another.

Where, TSACKpkt is time required for SACK Packet to travel from one node to another.

Step 7: Set an average Predefined Threshold value for IRTT as RTT. Maximum marginal delay ‘į¶ is the delay that can be added in maximum IRTT to set threshold value.

Step 8: Set an average Predefined Threshold value for Per Hop Delay (PHD) between nodes.

$$PHD = Max\ (TDatapkt \qquad (3)$$

Step 9: For each packet and for each group of 3 consecutive nodes, compare RTT,

```
Loop while (not end of simulation)

{

If (IRTT (N1, N2, N3) > RTT)
{
N1 Reports N2 and N3 as malicious.
If (TDatapkt (N1, N2) > PHD)

{
Network is not safe, node N1 is malicious. Terminate data transmission.

}
If (TDatapkt (N2, N3) > PHD)
{
Network is not safe, node N2 is malicious. Terminate data transmission.

}
}
Else
Network Is Safe. }//end while
```

V. SIMULATIONS AND RESULTS

Our simulation is conducted using the simulator developed by us in netbeans7.0.1 and JAVA – jdk1.0.7.0.45. We have generated network of 9 nodes. Designate source node and destination node, then we have to find path between this source and destination nodes. After obtaining the routing path, randomly any one node except source and destination can be set as malicious node. Malicious node will hold each incoming packet for some seconds with it. We have given the delay for malicious node in-between 3 to 9 seconds.

VI.CONCLUSION AND FURTHER RESEARCH

MANET is vulnerable to various attacks due to its open medium and wide distribution of nodes. In this paper, we implemented Secure ACK system to overcome weaknesses of existing systems. Proposed system works efficiently in presence of misbehaving node and instantly detects such node. The malicious activity detected in this paper is about malicious delay in packet transmission. System detects Misbehavior of any node in the network using Secure ACK algorithm within less time and stops data transmission. So, the misbehaving nodes would not be able to damage network thereafter.

REFERENCE

[1] I. Hatware, A. Kathole and M. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing," International Journal of Emerging Technology and Advanced Engineering, vol. 2, February 2012.

[2] Rasika Mali and Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study," International Journal of Scientific & Engineering Research, vol. 6, Issue 8, August 2015.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, 2000, pp. 255-265.

[4] N. Nasser and Y. Chen, "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network," in Proceedings of the IEEE International Conference on Communications, Glasgow, Scotland, pp. 1154–1159, June 24–28 2007.

[5] Arockia Rubi and Vairachilai, "A Survey on Intrusion Detection System in Mobile Adhoc Networks," International Journal Of Computer Science And Mobile Computing, vol. 2, issue 12, pp. 389-393, December. 2013

[6] T. Anantvalee and J. Wu. "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless / Mobile Security, New York: Springer-Verlag, 2008.

[7] I. Hatware, A. Kathole and M. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing," International Journal of Emerging Technology and Advanced Engineering, vol. 2, February 2012.

[8] Rasika Mali and Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study," International Journal of Scientific & Engineering Research, vol. 6, Issue 8, August 2015.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, 2000, pp. 255-265.

[10] N. Nasser and Y. Chen, "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network," in Proceedings of the IEEE International Conference on Communications, Glasgow, Scotland, pp. 1154–1159, June 24–28 2007.