IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

A Study on Detection of Misbehaving Nodes in Ad Hoc Routing

Monika Jatiwal[1], Parul Tomar[2]

Dept. of Computer Engineering, YMCA University of Science & Technology, Faridabad[1,2]

Abstract: Adhoc network is a collection of wireless networks. Each node communicate in a radio communication range. A MANET is a group of multi-hop wireless adhoc networks. Each node transfer the message to the other node through the wireless networks. This network is not fully secured so there are more chances of attacker .The success of mobile adhoc network depends on people’s confidence in its security. To identify the malicious node different techniques are used. This paper is going to deal with the malicious node for secure data transmissions.

Keywords: MANET, Adhoc network, malicious node, data transmissions, wireless networks.

1. INTRODUCTION

Each device in a MANET is free to move independently in any direction, and change its links to other devices frequently. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. As the nodes are free to move, any node can join or leave the network at any time. As the wireless network works on dynamic topology, various types of problems arise in the maintenance and route construction among nodes in the network. The main aim of routing algorithms is to find the best path from source to destination. While sending packet it may also happen that the any one of the node in between source to the destination node did not send the acknowledgement to the source node. Then that node is said as malicious node. So various techniques are described to identify that malicious node.

NODE BEHAVIOURS
Isha V. Hatware, Atul B. Kathole ,the nodes which creates dysfunction and damage other nodes are called misbehaving nodes. There are two types of misbehaving nodes such as malicious nodes and selfish nodes. Selfish nodes do not intend to directly damage other nodes, but also do not cooperate battery life for their own communications. But malicious nodes aim at damaging other nodes and they do not give priority to saving battery life.

2. REALATED WORK

TECHNIQUES USED FOR DETECTING MISBEHAVING NODES IN MANET
In MANET each node is dependent on cooperation with other nodes in order to forwarding and routing packets. The intermediate node in MANET are used for packet forwarding but if these nodes are misbehaving nodes then they can alter or delete packets. So various techniques are used for identification of misbehaving nodes.

Watchdog and pathrater gives the model WATCHDOG that improve throughput in the MANET in the presence of selfish node or malicious node. Watchdog overhear communication medium and it checks whether the next node is forwarding the packet faithfully or not. And it maintains a buffer. The packet id is removed from the buffer when the watchdog overheard that the same packet has been forwarded by the next-hop node over the communication medium. If a packet has remained in the buffer for longer than a certain time period, this mechanism marks the next-hop neighbor as misbehaving.

The Pathrater mechanism will help in finding the alternate path for transfer of packet.
Fig.1 shows the watchdog operation

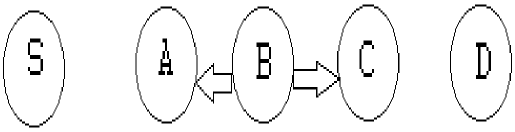

Fig.1

DOI10.17148/IJARCCE.2017.6679

From Fig.1 assume that source S wants to send packet to destination D. So there exists a path from S to D. Node A receives data packet from S. A send data packet to B and A keeps the copy in its buffer. A send the packet to C ensuring the B will forward the packet. If the packet is heard by B and it is identical to what it has in its buffer, this indicates that B has forwarded the packet to C. Now packet will be removed from the source node buffer. If a data packet remains in the buffer for a long period of time, the watchdog module accuses the next hop neighbor of misbehaving. If the packet is not compared with the packet of the source node buffer within the specific time period, the Watchdog adds one to the node B's failure counter. If this counter exceed the threshold, node A concludes that node B is Malicious and report this to source node S.

M. S. Alnaghes and F. Gebali, gives IDS that determine whether the data is under attack or not. IDS can be classified into two categories network-based IDS and host-based IDS. A network-based IDS runs at gateway of network and captures and monitors the data at the network. A host-based IDS relies on the operating system and it monitors the data generated by programs and users.

Rasika Mali, Sudhir Bagade introduced EXWATCHDOG IDS that ExWatchdog is an extension of watchdog. Its function is detecting intrusion from malicious nodes and reports this information to the response system. Watchdog resides in each node and is based on overhearing. A serious problem arises when the node that is overhearing and reporting itself is itself malicious, and then it can cause serious risk on network performance

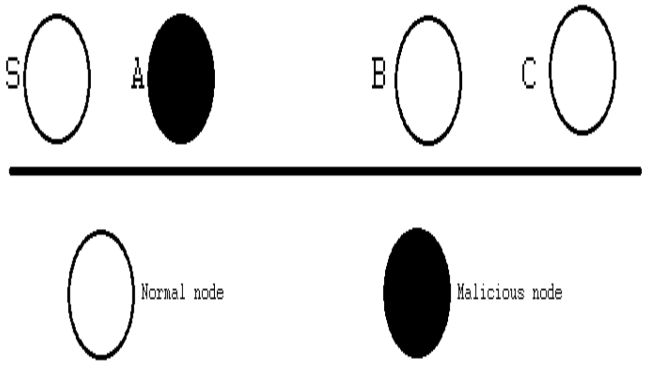

Fig.2

In the Fig.2 node A can report that the node B is not forwarding packets in fact it is forwarding. This will cause S (Source) to mark B as misbehaving when A is the real culprit. ExWatchdog maintains a table that stores entry of source, destination, sum that is total number of packets the current node sends, forwards or receives and path. Hence it can detect if nodes wrongly report other nodes as misbehaving. The main feature of this system is that it can discover malicious nodes which can break the network by wrongly reporting other nodes as misbehaving. This system fails when malicious node is on all paths from specific source and destination.

Sumiti, S. Mittal gives the confidant protocol which consists of monitor, trust manger, path manager and reputation system. In this all nodes monitors all the neighboring nodes within their radio range. Each node continuously monitors all its nodes in its vicinity. If any suspicious node is deleted than details of the event are passed to the reputation system. Reputation system modifies the rating of the suspected node. If the rating of a node in the table has reduced to fall out a tolerable range then the Path manager is called for action. ALARM messages are sent by the trust nodes. The Monitor manager of a node to warn others of malicious node observes the next-hop neighbor's behaviors using the overhearing technique. When a node finds a node as misbehaving node, it informs all neighbouring nodes and they too do not use this node.

S.Tamilarasan and Dr.Aramudan , suggested OCEAN protocol , in this protocol, every node maintains rating for each neighboring node and monitors their misbehavior through promiscuous mode. In this, protocols tracks misleading routing misbehavior. When a node forwards packet, the module fills the packet checksum. The OCEAN protocol overhear the behavior of the next-hop neighbor node. Then it applies the overhearing technique, if it does not hear the neighbor to forward the packet within a particular time period, Neighbor Watch registers a negative event against the neighbor node and removes the checksum from its buffer. On the other hand, on overhearing a forwarding attempt by the neighbor, Neighbor Watch compares the packet to the buffered checksum, and if it matches, it treats the packet as not having been forwarded. These events are communicated through the RouteRanker, which maintains rating of the neighbor nodes.

DOI10.17148/IJARCCE.2017.6679

In RouteRanker, every node maintains ratings for each of its neighboring nodes. The rating is initialized to natural and is incremented and decremented on receiving positive and negative events respectively from the Neighbor Watch component, when the absolute value of the negative decrement is larger than the positive increment. Once the rating of a node falls below a certain threshold, Faulty Threshold, the node is added to the faulty list.

Wenjia Li, Anupam Joshi, As per the authors TWOACK is neither an enhancement nor a Watch-dog based scheme. It aims at resolving the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaviour by sending acknowledgement through every data packets transmitted over each three consecutive nodes through the path from the source to the destination. After retrieval of a packet, each node that is two hops away from it throughout the route is required to send back an acknowledgement packet to the node down the route.

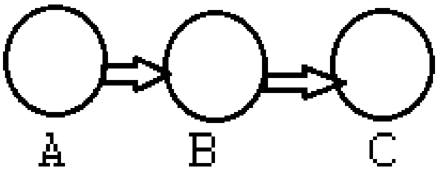

Fig.3

The working process of TWOACK is demonstrated in Figure 3 node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C then generate a TWOACK packet, which contains reverse route from node A to node C, and then through that route it sends back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

TWOACK scheme successfully solves both the receiver collision and limited transmission power problems that were posed by Watchdog. However, the acknowledgement required after transmission of every data packet creates a huge network overhead. Nature of MANETs due to the limited battery power, and such redundant transmission process can easily degrade the life span of the whole network.

AACK is somewhat similar to TWOACK.AACK is an acknowledgement-based network layer scheme which is a combination of a scheme call and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining the same network throughput. Both TWOACK and AACK suffer from the same problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets. Both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

Indhumathi.J, Prem Jacob.T proposed Fast random key algorithm in which network is assigning TTL. The source will send the data packet to the destination that network monitors all the node detail. And the network continuously update the key of each node for data transmission. If anyone of the node does not send acknowledgement to previous node then network will identify that misbehavior node based on primary key and inform to source node. Here the acknowledgement is must, based on this only it will identify the malicious node.

The techniques used in Fast random key are
1. Path selection
2. Acknowledgement
3. Buffer level

Path selection:
Each node in the network is assigned a key. The message is transferred to its neighbor node which is specified with the key. Through that only data will be transferred from source node to destination node.

Acknowledgement:
Acknowledgement is send to every node after receiving the data packet. Based on this only the sender is known whether the destination get the packet message or not. It uses the encryption method for secured transmission and the node will get acknowledgement from its previous neighbor node, which is already transferred the data packet.

DOI10.17148/IJARCCE.2017.6679

Buffer level
When the source will send the message to destination, the Time to Live (TTL) is assigned to network. Within the specified time period, each node should get the acknowledgement after reaching to the destination. If it not getting any acknowledgement within that specified time period then it is noted by the monitor. The Monitor sends the report to the source. Based on the monitor information, the malicious node is identified.

Comparison

Techniques	**Type of misbehavior**	**Key mechanism**	**Advantages**	**Limitations**
Watchdog	Drop data packets	Listen to its hop transmission	Improve throughput with presence of malicious node	Limited transmission power, False misbehavior report
Ex-watchdog	Drop data packets	Detects a node that sends false report	Solves problem of false misbehavior report	Limited transmission power, Ambiguous collision
TWO ACK	Acknowledgement packet delay	Acknowledge data packet transmitted over three consecutive nodes	Detects miss- behaving links	Adds overhead in the network
IDS	Drop data packets	Detects misbehaving nodes	Improve system efficiency	Cannot detect DOS attacks, agents disconnected due to link breakage
CONFIDANT	Drop data packets	Listen to its next hop transmission	Avoid misbehaving nodes	Limited transmission power, False misbehavior report
Fast Random key	Acknowledgement packet delay	Network monitors the nodes	Detects misbehaving nodes in less time as compared to TWOACK	False misbehavior report

3. CONCLUSION

The Dynamic nature of the MANET is a major challenge to maintain the frequently changing topology of the network. So there is more possibility of attacker and misbehaving node. When misbehaving nodes participate in the route discovery phase but refuse to forward the data packets, the performance is degraded severely. In this paper we studied the various techniques to detect the misbehaving nodes.

REFERENCES

[1] Isha V. Hatware, Atul B. Kathole, Mahesh D. Bompilwar" Detection of Misbehaving Nodes in Ad Hoc Routing" IJETE, Volume 2, Issue 2, February 2012
[2] Rasika Mali, Sudhir Bagade," Techniques for Detection of Misbehaving Nodes in MANET: A Study", International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015
[3] Sumiti, S. Mittal "Identification Technique for All Passive Selfish Node Attacks in a Mobile Network," International Journal of Advance Research in Computer Science and Management Studies, vol. 3, Issue 4, Apr. 2015
[4] M. S. Alnaghes and F. Gebali "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks," In Proceedings of Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing, Konya, Turkey, 2015
[5] S.Tamilarasan and Dr.Aramudan," A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System" IJCSNS, VOL.11 No.5, May 2011
[6] Wenjia Li, Anupam Joshi (IEEE Senior Member), and Tim Finin Coping with Node Misbehaviors in Ad Hoc Networks: A Multi- Dimensional Trust Management Approach. Eleventh International Conference on Mobile Data Management, IEEE 2010.
[7] Zaiba Ishrat "Security Issues, Challenges and Solution in MANET," International Journal of Current Science and Technology, vol. 2, Issue 4, Oct. - Dec. 2011
[8] Usha Sakthivel and S. Radha," Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, 2011
[9] Indhumathi.J, Prem Jacob.T," Identification of Misbehaviour Activities in Mobile Adhoc Networks", IJCSIT, Vol. 5 (2) , 2014

DOI10.17148/IJARCCE.2017.6679