International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Detecting Malicious Nodes for Secure Route Discovery in MANETs

Zalte S. S.[1], Dr. Ghorpade V. R.[2]

[1]Vivekanand College, Kolhapur, India

[2]Professor, D. Y. Patil College of Engineering and Technology Kolhapur, India

Abstract: ***In Today's world secure transmission of data is ubiquitous need. In MANET secure route discovery and secure routing of data plays an important role in data transmission. Because of it's dynamic topology, infrastructure less and openness, lots of intruders or malicious nodes getting a big opportunity to insert themselves as one of the legitimate nodes in the network. By taking this advantage they break down network performance of their malicious behavior. The major challenge is to secure route instead of data. Actually there is no fun to protect data rather than to protect route if route containing malicious nodes and packet is dropped by any of intermediate nodes due to one or another reason. In our paper we detect malicious nodes are restricted from router selection in the future by other nodes in network for secure data transmission.***

Keywords: Security, malicious nodes, MANET, legitimate nodes, secure data transmission

1. Introduction

Mobile Ad Hoc Networks (MANETS):-In manets nodes are communicating with each other without any central administration, a set of wireless mobile nodes that establish their own network dynamically on the fly. It is a temporary infrastructure less network. Because of its dynamic topology, infrastructure less and openness, lots of intruders or malicious nodes getting big opportunity to insert themselves as one of the legitimate nodes in the network. Different types of attacks mounted by the malicious attacker.

1) An attackers (internal or external) misleading two non-neighboring nodes into establishing a neighborhood relationship.
2) An attacker (internal or external) tricking a legitimate node to believe that an adversarial node (internal) is its neighbor, although it is not. The above attack types can have variants that involve a higher number of adversarial nodes.[3]

By taking this benefit they break down network performance by deploying their overwhelming malicious activities. Malicious activity is a specific activity which is projected to cause destruction to computing resources or communication network.

We summarized some following malicious activities.

1) Packet dropping:-Malicious nodes can drop all or selective packets.
2) Eavesdropping:-This attack is passive in nature. Attackers intercept communication and get control of secrete data.
3) Session Hijacking:-Here attacker can gain control of communication between legitimate nodes and retrieves
4) Confidential information.
5) Malicious node entering:-Without authentication malicious node can participate in network communication.
6) Link break:-Two valid nodes cannot communicate with each other because malicious node is between them.
7) Fabrication:-In network communication non authentic nodes can add fake data to system.
8) Replay attack:-In this attack attacker captures valid messages and resend them.
9) Fake routing:-Malicious nodes advertise itself that it has best route to the destination in order to capture packets.
10) Others:-There are many other malicious activities like stealing information, modification of message contents, and delay of packets. [1][2]

In MANET a new set of non-trivial challenges to security design because of various other features like mobility of nodes, promiscuous mode of operation, restricted processing power , battery, bandwidth and memory.

For MANET the following fundamental requisites are listed below.

1) Malicious Node Detection-Secure routing protocol must be able to identify the presence of malicious nodes in the network and should restrict participation of such nodes in the routing. If malicious nodes present in the route the routing protocol should select paths that do not include such nodes.
2) Correct Route Discovery-routing protocol should able to find out the correct route between source and destination.
3) Confidentiality about network topology-Attacker may try to study traffic pattern by knowing network topology. The information disclosure attack may lead to the discovery of network topology by malicious nodes.
4) Stability against attack-After active or passive attack routing protocol must be able to regress to its normal operating state within a finite amount of time. It should take care that there is no permanent disruption in the routing process [4].

2. Related Work

In [5] trust based forwarding scheme. Here each node contains neighbor trust counter table. Each intermediate node checks validity of digital signatures of the rep packet if not valid it drops otherwise it signed it and forward to next node.

The source node verifies first id of the route which is stored in rep packet if it is valid it checks digital signatures of all intermediate nodes. If they are valid trust counter values increases otherwise it decrements value of trust counter. If a trust value greater than the threshold value node is valid, otherwise it is malicious. Authentication performed by the route reply packet by cryptographic computations which in current route.

In [6] here author keeps track of two tables, sequence table and status table of its neighbor. Sequence table (SnT) is used to maintain the neighbor node's id and status table (ST) is used to maintain the node's status to check whether it is a normal or malicious node. Node declared malicious if Dst_Seq present in the RREP message and seqno present in it's table greater than threshold value. Source node also maintains flags table. The status of flag table is maintained by adding flag to each node which is used to detect a black hole attack...

In [7] Author proposed cooperative bait detection scheme (CBDS), that combine the advantages of both reactive and proactive defense architectures. It comprises three steps. In initial bait step with the cooperation of one hop adjacent node to detect whether malicious node is present in reply route. In the second step with the help of reverse tracing process it detects route which contains malicious node and malicious activity. After proactive defense next step is reactive defense in this step by using a threshold value of PDR under the control of time we can check still malicious nodes present in network or not. Threshold value adjusted upward if malicious node presents otherwise threshold value will be lowered.

In [8] Author proposed mobile secure neighbor discovery protocol to protect against wormhole attack. This module based on ranges when nodes are moving. Rigid graph is produced according to no. of ranges which is used to identify expected range and actual range. Packets are authenticated by using message authentication code and integrity achieve through hashing of nonce. Determination of wormhole attack is present done by analyzing ranges and travelled distances.

In [9] Author proposed SEDINE FOR static multi hop wireless network. It consists of two phases fist is a neighbor discovery phase. In this phase by using the first hop neighbor and second hop neighbor list algorithm prevent two non-legitimate nodes to become neighbors. Second phase is neighbor verification determines dropped verifier and link correct which is used to build secure path.

In [11] author proposed mobile agent method which is used to verify whether participatiNG NODE IS REAL NEIGHBOR OR FAKE NEIGHBOR Mobile agent keep neighborhood information and inconsistency checker find out abnormal activities of nodes. Mobile agent confirm particular node is attacker or not by visiting node and verifying information about the packets and location in the network.

In [12] Here author detect and prevent malicious node from participation in network by calculating ratio of no of packet loss and no of packets sent by node.

3. Proposed Algorithm

Aim of the proposed algorithm is to detect malicious nodes and prevent them in the routing path selection to maximize throughput and packet delivery ratio. The proposed algorithm consists of following main steps.

Step 1: Generation of 50 nodes in mobile adhoc network environment
Step 2: For each node pair of public and private key generated.
Step 3: Generate packet request for a neighbor to check whether that node is neighbor or not.
Step 4: Then neighbor nodes notify that particular requested node is our neighbor or not.
Step 5: If all node's reply is 'yes' then that node is not malicious. If any reply among them is 'no' then the node is malicious
Step 6: Once node found is malicious we set that node as inactive node.
Step 7: Here one node sending data to another node, it encrypts data by receiver's public key when data is received by receiver node it decrypts data by using its private key.
Parallel there is another flow in routing algorithm. There are following steps.
Step 1: In process of path selection when we select nodes in the particular path and we also check whether the node is active or inactive.
Step 2: In path selection only those routes are selected which contains only active nodes.
Step 3: If one of route containing inactive nodes, then that particular route is rejected in routing.

4. Simulation Results

In our paper, we used network simulator 3.14 for simulation. This simulator is most efficient in memory usage and performance wise also better in scalability than other simulator [10]. The simulation studies involve the deterministic small network topology with 50 nodes as shown in Fig.1. We simulate our secure neighbor discovery algorithm with NS3. In our simulation, mobile nodes move in a 500 meter x 500 meter square region for 20 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed is 20 m/s and the number of nodes are 50. We fix 2 nodes as attackers. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1.

Table 1: Simulation Settings

No. of Nodes	50
Area Size	500 X 500
Mac	802.11b
Radio Range	250m
Simulation Time	20 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Attackers	2 nodes
Speed	20m/s
Malicious nodes	8,10
Pause time	0
Propagation model	Two Ray Ground
Antenna Type	Omni directional antenna

4.1 Figures

In our paper, we compared two protocols first one is old aodv without detecting and preventing malicious attacks. In the second protocol we detect and prevent malicious nodes, which results increase in performance.

In Figure1. We plot the graph no. of times attacked against no. of attack detected. In our protocol we detect 100% attacks.

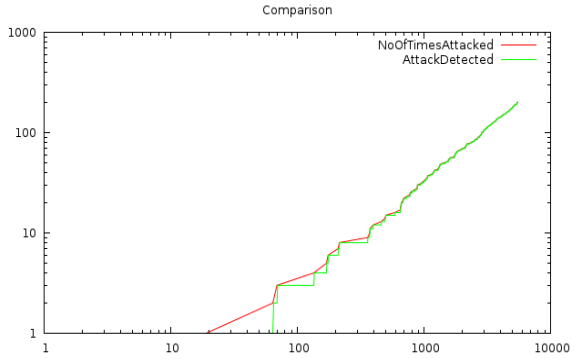

Figure 1: comparison of no of attacked vs. attack detected

In Figure 2. After preventing the malicious nodes in routing we get an increased packet delivery ratio and throughput.

Packet Delivery ratio=No. of packets received successfully / Total number of packets transmitted.

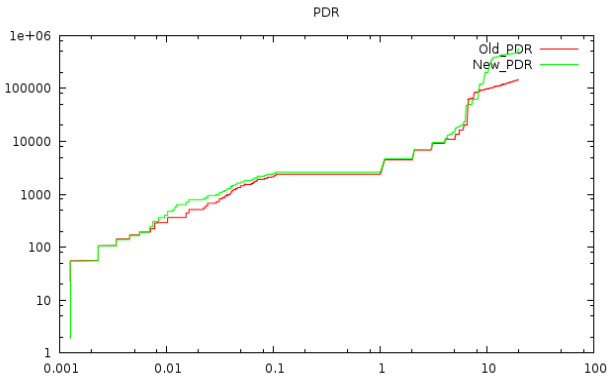

Figure 2: comparison of packet delivery ratio

Figure 3. Shows the throughput of old aodv protocol against our secure neighbor discovery protocol.

Throughput means no of total packets received within a particular time slot. Red line shows throughput of old aodv and green line shows throughput of new aodv.

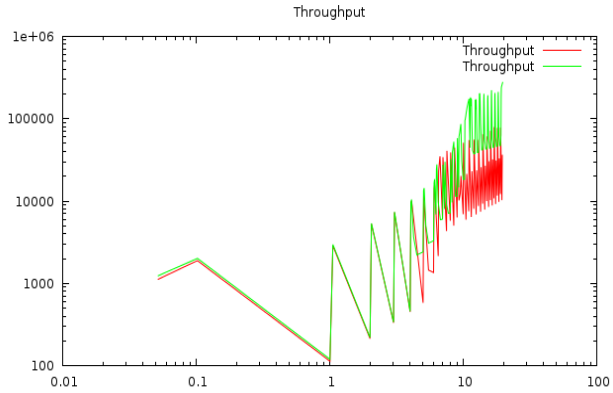

Figure 3: comparison of throughput

5. Conclusion

From above graph it is conclude that to allow only legitimate nodes to participate in routing and detect malicious nodes rather than trying to detect malicious nodes after their participation in routing results positive increment in PDR and throughput.

In next module we will provide security to data packets. Security is a boiling research topic and has to be taken into account in the design of solutions for MANET.

References

[1] Shringar Raw1, Manish Kumar1, Nanhay Singha, "Security Challenges, Issues and Their Solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, pp.95-105, September 2013.

[2] Radhika Saini, Manju Khari, "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network", International Journal of Computer Applications (0975 – 8887)Volume 20– No.4,pp.18-21, April 2011

[3] Pascal Lafourcade, David Basin, Srdjan Capkun, Jean-Pierre Hubaux ,"Secure Neighbor Discovery: A Fundamental Element for Mobile Ad Hoc Networking",IEEE,pp.1-7, February 2008.

[4] C.Siva Ram Murthy,B.S. Manoj,"ADHOC WIRELESS NETWORKS ARCHITECTURES AND PROTOCOLS", ISBN 978-81-317-0688-6,Pearson Education,

[5] A.Rajaram, Dr. S. Palaniswami, " Malicious Node Detection System for Mobile Ad hoc Networks ", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 77-85,2010.

[6] Reena Sahoo, Dr.P.M.Khilar, " Detecting Malicious Nodes in MANET based on a Cooperative Approach', IJCA Special Issue on "2nd National Conference-Computing, Communication and Sensor Network" CCSN, pp.46-51,2011

[7] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, pp.65-75,MARCH 2015
[8] R. Stoleru, H. Wu, H. Chenji, " Secure Neighbour Discovery in Mobile Ad Hoc Networks", Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 35-42,2011
[9] Ness B. Shroff ; Saurabh Bagchi, " Secure Neighbour Discovery through Overhearing in Static Multihop Wireless Networks", Wireless Mesh Networks (WIMESH 2010), 2010 Fifth IEEE Workshop on 21 june Print ISBN:978-1-4244-7975-7 pp.1-6.2010
[10] Weingartner, E., Vom, L., Wehrle, K. (2009), "A performance comparison of recent network simulators", In: Communications, ICC'09. IEEE International Conference on (1-5).
[11] Nagesh Sindagi1, K Sundeep kumar2, Manoj Challa3, Ashwatha Kumar M4, "Secure Neighbor Discovery in Wireless Networks by Detecting Various Attacks", International Journal of Computer Science and Mobile Applications, Vol.1 Issue. 1, July- 2013, pg. 1-11 ISSN: 2321-8363
[12] G. S. Mamatha, Dr. S. C. Sharma, " A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS ", International Journal of Computer Science and Security, Volume (4): Issue (3) pp-275-284, July 2010 .