Detecting Selfish Node over the Active Path using Neighbor Analysis based Technique

Sumiti[1], Dr. Sumit Mittal[2]

[1, 2]MM University, MMICT & BM (MCA), Mullana (Ambala)

Abstract: ***In this work, a nearest neighbor analysis has been performed to detect the selfish nodes in the active path and to generate a secure path. The existing AODV protocol is modified and a new bit is taken to define the trustful status. If status is 1, then node is valid, otherwise the node is selfish node and no communication is performed over that node. As the communication is performed, each node is analyzed by its neighboring nodes and builds a trust table. The reply status is 0 (by default) as the successful replied is received by a node, the value in the table changed to 1. Now the protocol checks the shared table and identifies the reply status. If the reply status is greater than the threshold value, the node is taken as the valid node and communication over that node is performed. This work has been implemented using NS-2.29 simulator and results shows that this technique is able to detect almost 90% selfish nodes in the active path.***

Keywords: MANET, Selfish Node Attack, Nearest Neighbor Analysis

1. Introduction

Mobile ad hoc network (MANET) is a wireless network and does not depend on the already existing infrastructure because wireless nodes are capable of freely and dynamically self-organizing in to the network and due to the reason network topology changes fastly. In such networks, there are different types of nodes and each node is capable of communicating directly with any other node residing within its transmission range. Mobile ad hoc network has few problems like nodes moves randomly, dynamic network topology and route changes; so there is a huge probability of different types of attacks and packet losses. In the networks different types of attacks are attacked by the attacker known as malicious nodes and critical nodes. Malicious nodes are those nodes that harmfully affect the network and other nodes e.g selfish nodes. Attacks in Mobile and Ad hoc network (MANET) can be classified as:

- Passive Attack
- Active Attack

In the passive attacks, the attacker only detects the data which is exchanged in the network, and use it for their own use without modify it or in other words only eavesdropping of data. In a passive attack, the attacker's motive is just to gather information about the network and the communication pattern. But in the active attacks, the attacker modifies or changes the data which is transmitted in a network. The attacker has full control on the packet and can even inject or drop the packet. In MANET attackers are also known as comprised nodes. Malicious or compromised nodes are those nodes in the network which are responsible for the active attacks or damages the other nodes. Malicious nodes can easily perform attacks by alter the information in the protocol field, to destroy the transfer of the packets, to deny access among the legal nodes.

In the MANET there are various types of attacks but we have focused on the selfish node attack. Selfish nodes are those nodes when the nodes receive the data and do not send to next node; instead they use them to store their battery lifespan, which they use for their own communications. The efficiency of the network is greatly reduced by the selfish nodes because they do not participate in the network operations. Generally, it is easier for a node to become the selfish node e.g. save resources for itself and ignore all packets (data and control) that are not destined for it and does not forward packets to next node. But some well-behaved nodes in the network might not be required to forward data packet. Examples of those scenarios are listed as the following:

1) The node is located at the edge of the network. At that location, the node does not have any other node to forward data packet.
2) The network is already mature where all routing to every possible destination has been established. A new node then enters the network and wishes to use the network to establish communication to another node. As long as there is no link error, there is no change in the routing table. The new node does not get any RREQ packet. As a result, the new node does not be requires to do data forwarding.

In this paper we have focused on detection of the selfish nodes only active path. Below given figure shows about the active and passive paths.

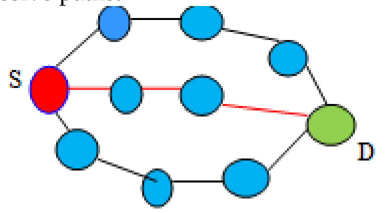

Figure 1: Shows the active and passive path

🔴 Source node
🟢 Destination node
🔵 Simple node
— Passive path
— Active path

2. Related Work

The security problem and about the cooperation between the nodes in network have been studied by different researcher in the ad hoc network.

Watchdog and path rater [16] proposed an approach to detect and isolate the misbehaving nodes. In this, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes. However, it has the demerit of not penalizing the malicious nodes.

Buchegger and Boudec[15] suggested that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially.

Singh et.al. [3] proposed the Detection and Prevention of Blackhole Attack in Mobile Ad Hoc Network and quite successful against black hole attack.

Chaba et.al. [4] proposed a Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET.

Chaba et.al [5] have identified the mechanism for Detection of Malicious Packet Dropping Based DDOS Attack in MANET. However, none of these protocols are very effective solution against PDDoS attacks in MANETs.

Poonam [8] proposed an opinion based cooperative trust model to improve the performance of network, particularly in the presence of malicious nodes. In the proposed model, each node determined the trustworthiness of the other nodes with respect to behavior observed. It calculated the direct trust by the information obtained independently of other nodes and indirect trust information obtained via opinion of other nodes.

Poonam [9] proposed a novel method to enhance security in both phases. Author presented the design of a routing protocol based on trust, which ensures secure and undisrupted delivery of transmitted data. An end to end encryption technique has used to self encrypt the data without the necessity of a cryptographic key.

Mobile Ad hoc networks are characterized by wireless connectivity, continuous changing topology, distributed operation and ease of deployment. The work proposed contributes to detect the black hole attack using Modified Associatively Based Routing protocol (MABR) which is the modification and improvement of ABR [10].

Poonam [11] proposed a novel opinion based trust-aware routing protocol (OBTRP) for MANETs to protect forwarded packets from intermediary malicious nodes. In the proposed model, each node determines the trustworthiness of the other nodes with respect to behavior observed. It calculated the direct trust by the information obtained independently of other nodes and indirect trust information obtained via opinion of other nodes.

3. Existing System

One of the biggest issues in mobile ad hoc network is that the topologies change dynamically because of the node movement. Not only this, even the nodes usually have no predefined trust factor between each other. And another biggest issue is the technical properties of regular nodes itself like less energy of nodes. This property is most critical because malicious nodes try to copy this and make it difficult to distinguish between regular node and malicious node. A malicious node from their behavior disturbs the network operations and wastes the resources of regular nodes. But intelligent malicious nodes elaborately choose a frequency at which they cooperates the regular nodes.

4. Proposed Technique (Nearest Neighbor Analysis using bit change based technique)

In this proposal, each monitoring node operates in promiscuous mode and monitors both data and control packets that are send around within its receiving range. Each monitor node keeps record of its each neighboring node. In this framework, a specific table is use for store the information about the neighboring nodes. An extra field has added in the table as the following:

1. Last Action
2. Last Request
3. Status

1. Last action of the neighbor node is that the last time seen of neighbor node for contribution or providing services to the network.
2. Last request of the neighbor node is that the last recorded time of the neighbor node for last seen utilization or requesting for services from the network. Monitoring node updates these two fields every time, when take any action for promiscuous mode.
3. Status is the current behavior of the neighboring node that is detected by the monitoring node. The initial status for any unknown node is set to zero and later on changed according to their suspicious and behavior.

Whenever a monitoring node hears a request from its neighboring node for forward a data packet, first it checks the time difference between last request and last action of the requestor. If it is within a threshold value means (TTL=1), then called Action Hold off Value. If the value difference exceeds the threshold, the status for the node has been set to suspicious and for find out the status of the suspicious node a special scenarios is used. In this testing, a fake RREQ packet is broadcasted into the network. For minimize the traffic flooding in the network, only the node that receives the data forward request from the suspicious node is conducting this test. In addition, this fake RREQ packet passes through one hop (TTL=1). If it takes time more than (TTL=1) it means this node is the selfish node and if it takes less than (TTL=1) it means this node is the valid node. All monitoring nodes in the neighborhood that detect this potential misbehavior and waits for the suspicious node to rebroadcast the fake RREQ packet within a certain timeout. If it responds the RREQ packet, the status of the node is set to behave and the time of its last action is updated. If it discards the packet and does not respond, the monitoring nodes are labeled the suspicious nodes as selfish.

5. Algorithm

```
Selfish_node_detection ( NAmax , NAi )
{
// NAmax= maximum value of average retransmission numbers in the period //
// $NA_i = \frac{\sum_{j=1}^{n} NA_j}{n}$ , j=1,2,........n
 if (NAmax – Nai < Threshold)
 {
 N k = non-selfish node;
 }
 else
 N k = selfish node;
 if(NAj= = 0)
 {
 N k is fully selfish node;
 }
        }
```

Table 1: Simulation Parameter

Simulation Parameter	Value
Number of Nodes	50
Simulation Time	100 sec
Topology Size	700 X 700
Traffic Type	CBR (Constant Bit Rate)
Packet Size	512 bytes
Antenna Type	Omni directional Antenna
Routing Protocol	AODV
Queue Length Type	Drop Tail
Radio Propagation	Two Ray Ground
Total Packets	50
Channel Type	Wireless Channel
Network Interface Type	Wireless Phy

Performance evaluation is carried out using NS2. Nodes moves according to the two Ray Ground mobility model. And here aim is to implement AODV routing protocol for 50 nodes and sending CBR packets within random speed. First the CBR files and scenario files are generated and then using AODV protocol simulation is done which gives the NAM file and trace file. The mobile node is simulated with a velocity of 0-20m/s. It sends 300 CBR packets approximately. The performance metrics are throughput and energy.

Attacker Nodes are shown in Red color example 4, 38, 39, 14 and these nodes drops packets from their nearest nodes. Black blocks are shown in the screen shows the packet drops from the normal nodes. Since there is no security to define so packets are dropping during the route define because attacker's nodes are present at nearest paths. For example: node 4 is dropping packet from the node 36, node 38 is dropping packet from the node 9 and node 39 from the node 40. For securely transfer data from source to destination node without dropping packets we consider Node 1 is server. And this server (1) checks communication within each node for securely data transfer without using computational assumption.

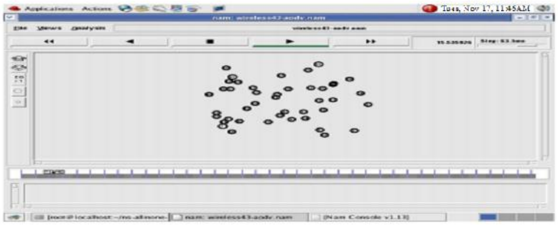

Figure 2: Normal simulated nodes

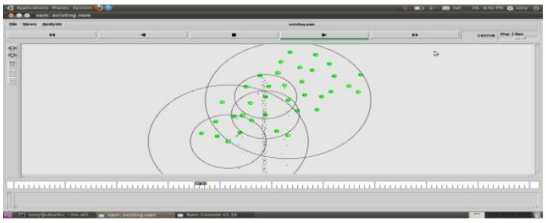

Figure 3: Selfish nodes dropping packets

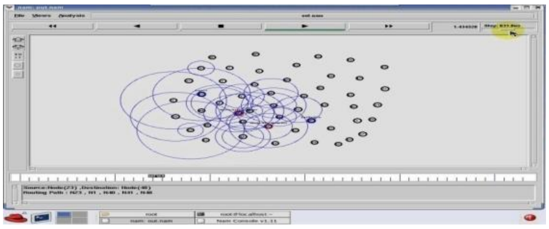

Figure 4: Showing secure route

According to the figure 5, Source node 0 sends data to Server Node 1. Black dot is shown between 0 and 1. After this data communication checking is done between the black node 48 and 13. Then data communication checking is done between the black node 13 and 45. After communicate with these nodes in this path, a new routing path is selected from source to destination. Blue color nodes shows a new secure path for data transfer from source to destination node example 0—2---26—7—22---48 – 13 – 45 – 44. By using this path data is securely transfer without packet loss.

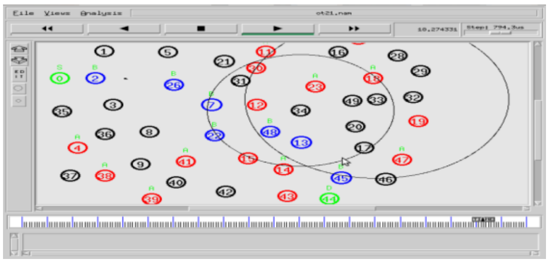

Figure: 5 Screenshot shows secure data transfer through the specified path without packet loss.

Below given figure shows the comparison of Packet Delivery Ratio (PDR) for Selfish AODV (four nodes acts as selfish) and Normal AODV (No selfish node). Graph for Normal AODV shows that there is no any loss of data packets means no one node acts as a selfish node ie. 100% PDR and But graph for Selfish AODV shows that there is loss of some packets, all packets are not delivered. In this, some nodes act as selfish nodes. And these nodes find out with the help of our neighboring node based system for MANET to detect selfish node.

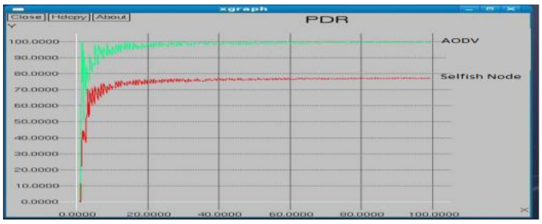

Figure 6: Shows the result

6. Conclusions

Mobile ad hoc network is a famous upcoming field of research with practical applications. Because there are many reasons of attacks like lack of regular security infrastructures, changing network topology and open medium of communication, which are not totally secured. The analysis shows the real challenge of this study is that the throughput performance depends on the number of paths in the network and the locations of malicious nodes. And the communication checking between nodes depends on the detection range (that a server is in the range of a sender and a malicious node). Simulation results shows the effect of network sizes, numbers of nodes and mobility speed that helps to understand the impact of the packet dropping attack and its mitigation.

References

[1] R.Gopal, V.Parthasarathy, A.Mani, “Techniques to Identify and Eliminate Malicious Nodes in Cooperative Wireless Networks”, IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), Jan 2013.

[2] Dipali Koshti and Supriya Kamoji, “Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks” International Journal of Soft Computing and Engineering (IJSCE) , Volume-1, Issue-4, September 2011.

[3] Yudhvir Singh, Yogesh Chaba, “Detection and Prevention of Blackhole Attack in Mobile Ad Hoc Network”, In proceeding of IEEE International Conference on Advance Computing Conference, IACC 2009; March 6-7, 2009; pp 2668-2672.

[4] Yogesh Chaba, Yudhvir Singh, Preeti, “Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET”, Journal of Networks, Academy Publisher, ISSN: 1796-2056.

[5] Yogesh Chaba, Yudhvir Singh, Preeti, “Detection of Malicious Packet Dropping Based DDOS Attack In MANET”, Journal of Computer Science, ISSN 0973-2926; Vol. 3, Issue 2, Jan-Feb 2009; pp 959-964.

[6] Yogesh Chaba, Yudhvir Singh, Preeti, Deepak, “Performance analysis of various distributed denial of service based attacks in mobile adhoc networks”, IEEE International Conference on Advance Computing Conference, IACC 2009; March 6-7, 2009; pp 3228-3132.

[7] Preeti, Yogesh Chaba, Yudhvir Singh, “Review of Detection and Prevention Policies for DDoS attacks in MANETs”, In Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008) RIMT-IET, Mandi Gobindgarh; March 29, 2008; pp 56-59.

[8] Poonam, "Eliminating misbehaving nodes by Opinion based Trust Evaluation Model in MANET’s”, ICCCS’2011, Rourkela, Odisha, India, ACM 978-1-4503-0464-1/11/02.

[9] Poonam Gera, "Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANET’s", SIN’2010, Taganrog, Rostov-on-Don, Russian Federation, ACM 978-1-4503-0234-0/10/09.

[10] M.Shobana, "Geographic Routing used in MANET for Black hole Detection", CCSEIT-2012, Coimbatore, Tamilnadu, India, ACM 978-1-4503-1310-0/12/10.

[11] Poonam, "Misbehaving nodes Detection through Opinion based Trust Evaluation Model in MANETs", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), TCET, Mumbai, India, ACM 978-1-4503-0449-8/11/02.

[12] Preeti, Yogesh Chaba, Yudhvir Singh, “Distributed Denial of Service: Taxonomies of attacks and Countermeasures”, In National Seminar on ‘Enterprise Information Systems’ at Apeejay College of Management, Jalandhar; May 24, 2008

[13] Y. an Huang and W. Lee, “Attack analysis and detection for ad hoc routing protocols”, in Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), September 2004.

[14] S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in MOBIHOC'02, 2002.

[15] J. Mundinger and J.-Y. L. Boudec, “Analysis of a reputation system for mobile ad-hoc networks with liars," wiopt, vol. 00, pp. 41{46, 2005.

[16] L. Buttyan, and J. Hubaux, “Enforcing cooperation in self organizing mobile as hoc networks,” In Proceedings of IEEE/ACM Workshop on Mobile Ads Hoc Networks, Technical reportDSC/2001/046, EPFL-DIICA, August 2002.

[17] F. Kargl, A. Klenk, S. Schlott, and M.Weber, “Advanced detection of selfish or malicious nodes in ad hoc networks”, August 2004.

[18] Radhika Saini and Manju Khari, “Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network” International Journal of Computer Applications, Volume 20, No.4, April 2011.

[19] Jaswinder Singh and Ramandeep Kaur, “Towards Security against Malicious Node Attack in Mobile Ad Hoc Network”, IJARCSSE Volume 3, Issue 7, July 2013.

[20] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks” in The 6th ACM International Conference on Mobile Computing and Networking, 2000.

[21] Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network”, International Journal of Wireless Communication, ISSN 0974-9640, pp 885-890, (August, 2011).