MISROUTING ATTACK DETECTION USING TSM ALGORITHM

K.Jayabharathi[1], A.V.Sindhuja[2], C. Priyanka[3], K. Chitra[4] and Sanjay Kumar Suman[5]

[1]*Associate Professor, ECE, MNM Jain Engineering College, Chennai, India.*
[2]*Assistant Professor, ECE, MNM Jain Engineering College, Chennai, India.*
[3]*Associate Professor, ECE, MNM Jain Engineering College, Chennai, India.*
[4]*UG Student, ECE, MNM Jain Engineering College, Chennai, India.*
[5]*Professor, ECE, MNM Jain Engineering College, Chennai, India*

ABSTRACT

MANETs are widely used for communication purposes. Using MANETs is a win-win situation, this increases the communication between the nodes, but this will also, compromise on the security of the data being transmitted and the battery life constrain. This battery life becomes precious because since these are short living nodes, user cannot load these nodes with huge battery. This huge battery size will also hamper the movement of these nodes. This battery life is further wasted when there are many unwanted transmissions taking place. This will drain the battery power and render it useless too soon. Here we are going to deal with such an attack misrouting which will drain the battery power and make it useless. Misrouting will not only drain the battery power, it will unnecessarily waste the bandwidth also. A centralized node mechanism is being implemented here, all the distance information, traffic information and the delay information is being fed into the user nodes through the centralized mechanism. This will alert the user node when an intended data is not received well within the stipulated time.

Keywords: *TSM algorithm, mobile Ad hoc Network, certificate authority, maximum burst size, minimum burst size, large size low traffic, Large size high traffic*

1. INTRODUCTION

MANETs are adhoc type of networks which is used for immediate transmission [8]. This enables the user to send or receive information in sec by sec basis or in even smaller time difference. MANETs are very effective in sensing on a particular information or in collecting and receiving, with these many advantages MANETs also have a few disadvantages like battery constrain, memory capabilities , security etc. When the battery of the nodes is drained out completely the node becomes redundant. Thus the user is forced to change the nodes periodically for continued monitoring. Sometimes due to high level of data monitoring these nodes might drain out the battery and on the other hand sometimes a malicious user might drain the power in order to make the whole network redundant. This is said, when the security of the network has been compromised.

2. SECURITY ATTACKS ON MANETS

There are many attacks carried out on MANETs which are aimed at draining the battery power of the node, misrouting the data being transmitted, selective dropping / forwarding, flooding the network with unwanted requests [6].

2.1 Active Attack

Attacks which will modify or change the contents of the data being transmitted are called as active attacks. These kinds of attacks are very harmful to both the users at transmitting end as well as on receiving end. Since the receiving user will not receive the correct intended data, he will think that the transmitting node has being compromised and block that nodes. There are two possibilities for such a malicious data transfer, either the

transmitting node maybe compromised or a node in between the receiving node and transmitting node can act as a black hole. In the Fig. 2.1.1, S (source node is compromised and it is transmitting irrelevant data to receiving node

Fig-2.1.1 Unwanted data transmission

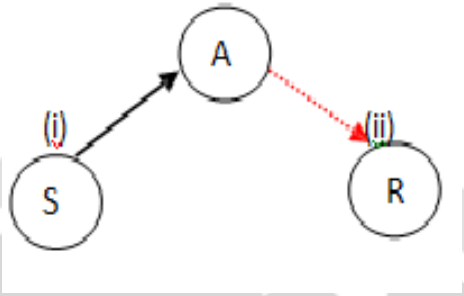

Fig-2.1.2 Compromised node data transmission

(R), in order to flood the network and waste the battery power of the receiving node. In the Fig 2.1.2, we see the original data to be transmitted is represented by the index (i), which the source node(S) thinks is being transmitted to the receiving node (R), but there is an Attacker node sitting in between these two nodes and will gather all the information and transmit its own similar random data. This will lead, R to think that S is being compromised and block it.

Another type of active attack is Misrouting. In this the attacker node will pose as a genuine node and will advertise a route table which is fake. This route table will have routes with short distances to all the possible nodes. The transmitting node will be led to believe that this is the shortest and efficient transfer mechanism and chose it. But the transmitted data will not be received by the user. Thus a lot of energy and bandwidth will be wasted.

2.2 Passive Attacks

Passive attacks are the hardest to identify and mitigate. As they remain passive without the slightest interference to the users. Such examples of passive attacks are eavesdropping and traffic analysis and monitoring.

- **Traffic analysis and monitoring**: with the pattern of traffic being transmitted the attacker will be able to predict the bursts of data being transmitted and launch attacks accordingly.
- **Eavesdropping:** The attacker will remain silent throughout the conversation between the users and will gather the important information such as private keys , passwords etc. This will be passed to the attacker who will easily invade the network with this data.

3. RELATED WORK

Many mechanisms have been proposed for the elimination of misrouting of packets. In [1], various possible attacks on MANETS are studied and for each possible attack various mechanisms like cryptography techniques are proposed. But since all the mechanisms might have a disadvantage, the computational time involved in cryptography is greater. In [2], various mitigation techniques for attacks such as intrusion detection scheme etc. In [3], a check facility is added to the neighboring nodes, these nodes will have to check all the ongoing transmissions

3.1 Network Model

Here we are considering a wireless mobile adhoc network with about 10 nodes (for our explanation purpose). Additionally to these 10 nodes, there is a authorized node, which will act as the centralized node with all the information. Data is sent to this authorized node from a few authorizing nodes deployed between the nodes. These authorizing nodes will transmit traffic related data to the authorizing node. The other route related

information is transmitted by the nodes themselves. These metrics are calculated by the Authorizing node and sent to nodes to avoid miscalculation. All these data are encrypted. These nodes will transmit data in bursts in various sizes where the maximum burst size if B_{MAX} and the minimum burst size is B_{MIN}.

3.2 Security Model

Here we are considering that all the nodes before start transmitting have been notified with the connection status of other nodes and the distance between the nodes. All the nodes are identified by metrics which are derived using the performance of the nodes in the previous transmissions.

4. PROPOSED SYSTEM

We are considering the data transmission at time slots T1, T2....Tn Sleep range

- **Identifying Metrics**: According the nodes behavior in the T1 time slot, the nodes are assigned some metrics like the Performance metric, Processing metric and the Time metric.
- **Performance metric**: With reference to the Packet delivery ratio and the Packet drop ratio. We assign every user a value in the range 0-1. For example if the packet delivery ratio is0.8 then the metric assigned will be 1. And thepacket drop ratio is 0.2 the metric assigned will be 0.1
- **Time metric:** is the parameter assigned to the variable according to the time it takes to deliver a packet and receive the acknowledgement.

4.1 Route Table and Traffic Transmission

All the nodes are transmitted data about the neighboring nodes and the laps between them (Cost of transmission). When the S intends to send data, it will know the size of the data it is going to transmit.

- **Variable data:** when the data being transmitted is going to be of varying sizes, i.e. Continuous data then the size is determined using a ± of 5%.
- **Fixed Data:** When the data size is fixed, then the S will know the size of data in bytes/sec.

4.2 Calculating Total Time Delay

Before the actual transmission starts, the total time involved in transmitting data between all the nodes under 4 condition is calculated.

- Large size low traffic.(LLO)
- Large size high traffic.(LHI)
- High size low traffic(HLO)
- High size high traffic (HHI)

4.3 Mechanism

Let us assume the following network model shown in Fig. 4.3.1. All the metrics of the nodes connected in the system is calculated with reference to the transmission in the T1 time slot. This data is sent over the network by authorized node, which will act as the information about all other remaining member nodes, authorized node to collect transmit and store. Assuming this a table transmitted to node 2 by node 3 (Table 4.3.1). Now node 1 wants to send and receive data from node 10, which is located at the other information obtained by the node 1 , it will calculate. This node 1 will receive the traffic information from the Authorized node.

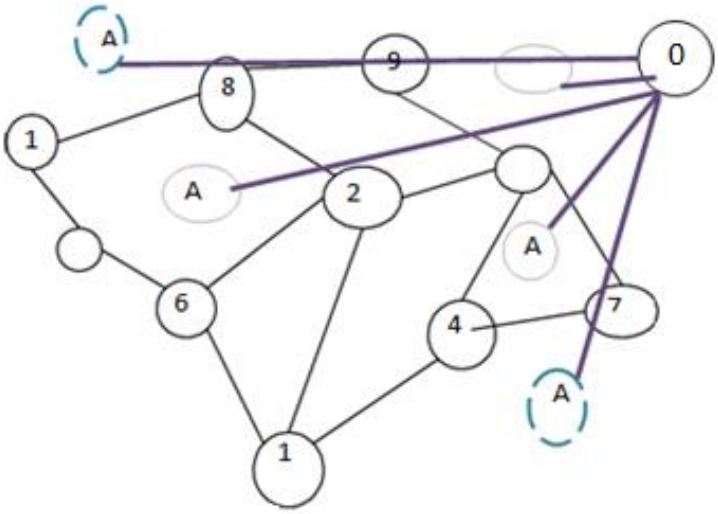

Fig-4.3.1 Network Model

Now at node 1 will chose the best path the metrics for each route and the time delay involved in transmitting data under the following conditions out of all these nodes and transmit data through it. The best path chosen is again sent to the authorized node. This authorized node will notify all the nodes in this path about the impending data transmission and the likely time when it will receive data [7]. The Calculations are as follows:

Table-4.3.1 Routing information transmitted to node 1 at Time slot T2

Nodes	Paths available	Cost	PaDR	PDR	PM	Ti			
						TLLO	THLO	THLO	THHI
Node 2	1-8-2 1-5-6-2	12 14	0.2 0.5	0.8 0.5	5micsec	1.5s	3s	4s	8s
Node 3	1-8-2-3 1-8-9-3	10 9	0.8 0.65	0.2 0.35		.			
Node 4	1-5-6-10-4 1-8-2-3-4 1-8-2-10-4	8 18	0.78 0.25 .	.	.	.			
Node 5	1-5	2	.	.	..	.			
Node 6	1-5-6	4	.	.	.	.			
Node 7	1-5-6-10-4-7 1-8-2-3-7 1-8-9-3-7	8 16 12	.	.		.			
Node 8	1-8	4	.	.					
Node 9	1-8-9	8	.						
Node 10	1-5-6-10 1-8-2-10	8 10	0.6 0.4	0.4 0.6	2mics 3mics	1.2s 1.25s	2.8s 2.4s	2s 1.5s	6s 6s

- $\mathbf{T_{HLO}}$ = burst size / total round trip time
- $\mathbf{T_{LLO}}$ = burst size / total round trip time delay
- $\mathbf{T_{LHI}}$ = burst size / total round trip time delay
- $\mathbf{T_{HHI}}$ = burst size / total round trip time delay

When the RTT for high traffic is to be calculated, the authorized node initiates packet transmission requests and acknowledgement packets from remaining (n-2) nodes. This will give an effect of a high traffic. Since the traffic due to data could be of various sizes of data, this is covered in the +_ 5% in the time instant of data receiving. From the given parameters in table 4.3.1 we identify that the path 1-5-6-10 are best. This information is passed to the CA, CA notifies the nodes 5,6 about the transmission that is to take place. It will also tell the nodes that when likely it will receive the packets. The nodes will wait for a maximum of 5microsecs for the packet, else send an alert signal to CA. CA with the help of Authorizing nodes will identify the nodes which is misrouting or trying to misroute and block that node from that transmission.

5 RESULT ANALYSIS

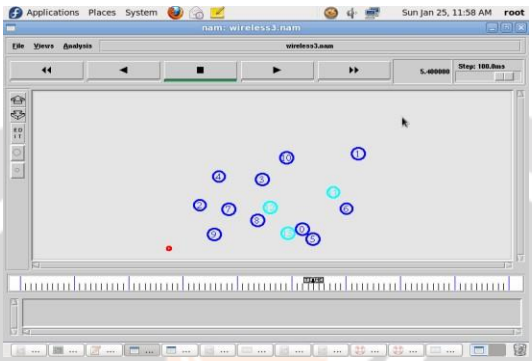

Fig-5.1 Node Deployment at T2

We have made comparative study of the throughput and packet delivery ratio of the normal transmission and transmission with the mechanism proposed and we have seen a considerable improvement in the performance.

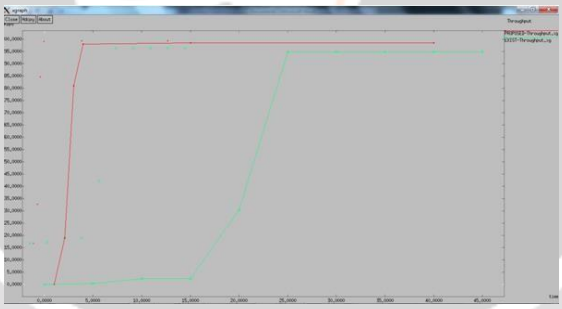

Fig-5.2 Throughput

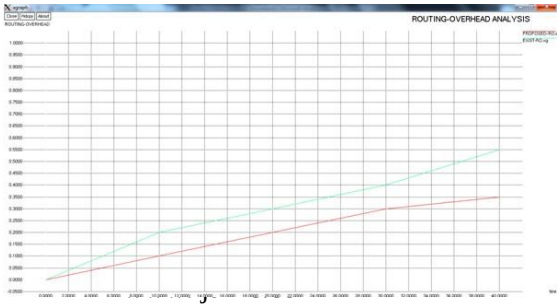

Fig-5.3 Packet Delivery ratio

6 REFERENCES

[1]. K.P .Manikandan, Dr.R. Satyaprasad and Dr.K. Rajasekhara Rao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks",, in proc of *(IJACSA)* International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011

[2]. Maulik H. Davda, Sheikh R. Javid , "A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes *"*, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 4, April 2014

[3]. E.S. Phalguna Krishna, I.D. Krishna Chandra, M. Ganesh Karthik ," Packet Misrouting Attacks in Multi Radio Wireless Networks: Detection and Countermeasure ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[4]. Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Adhoc Networks" Department of Computer Science, University of York.

[5]. Ramaswamy, Ning Weng and Tilman Wolf, Characterizing network processing delay, in proc of Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, Vol. 3, 2004.

[6]. P. Vimalrajkumar, K.Jayabharathi:" Major Packet Attacks in Adhoc and Multihop Networks: Detection and Rectifying", in proc. of National Conference on Recent Trends in Electrical and Communication Engineering (NCRTECE '13), 2013.

[7]. Jonny Karlsson, Laurence S. Dooley and Göran Pulkkis, "A New MANET Traversal Wormhole Detection Algorithm Based on Time and Hop Count Analysis", in open access journal, Sensors, Vol. 11, Issue 12, pp. 11122-11140, Nov. 2011.

[8]. Sanjay Kumar Suman, Dhananjay Kumar and L. Bhagyalakshmi, "SINR pricing in non cooperative power control game for wireless ad hoc network", KSII Transactions on Internet and Information Systems, vol. 8, no. 7, pp. 2281-2301, 2014.