Secure Data Communication for Mobile Ad Hoc Network Using Zonal Routing Protocol

S. Dhanalakshmi[1], Dr. M. Rajaram[2] , Dr. S.N. Sivanandham[3]
[1]Department of MCA, Selvam College of Technology, Namakkal, India
[2]Department of EEE, Government College of Engineering , Tirunelveli, India.
[3]Department of CSE, PSG Tech., Coimbatore , India.
E-Mail : [1] mecmca_hod@yahoo.co.in

Abstract **- Mobile ad hoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid of establish infrastructure. In Mobile Ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes in underlying protocol design, and lack of centralized monitoring and management point. The main aim of this work is to provide secure data transmission between the source and destination. The simulation is carried out for different number of mobile nodes using network simulator with the help of 1000 mobile nodes. We have compared this model with the existing models such as DSR and AODV. This model has shown the better results in terms of packet delivery, packet drop, and delay. The proposed model has dropped 19% of the packets even if network has five malicious nodes.**

Keywords **- MANET, ZRP, security, mobility, Mobile Ad hoc Network, AODV, DSR, Destination, Source, Delay.**

I. INTRODUCTION

In recent years, Mobile Adhoc Network(MANET) has received marvelous attentions due to self-design, self-maintenance, and cooperative environments. In MANET, all the nodes are mobile nodes and the topology will be changed rapidly. The structure of the MANET is shown in Figure 1. Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes are actively discovered the topology and the message is transmitted to the destination over multiple-hop[1]. Usually, the endpoints and routers are indistinguishable in MANET [2]. It uses the wireless channel and asynchronous data transmission through the multiple-hop. The vital characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes.

The end-nodes are enabling QoS such as end-to-end delay, packet-loss, throughput and secure data transmission [2]-[3]. The potential deployment of MANETs exists in many scenarios, for example in situations where the infrastructure is not feasible such as disaster relief and cyclone, etc. The MANETs have potential of realizing a free, ubiquitous, and Omni directional communication [3].

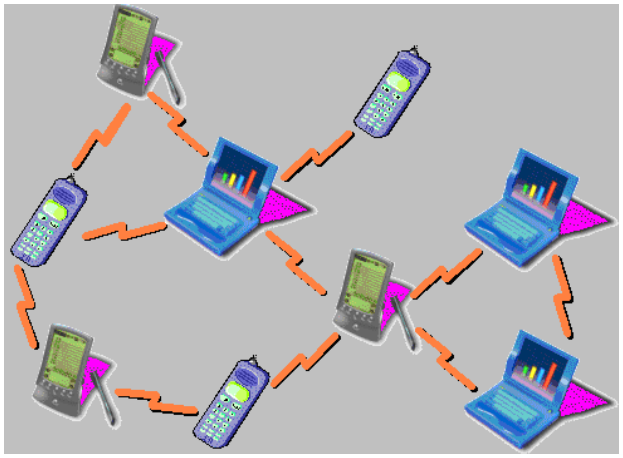

Fig.1. Structure of MANET

The wireless channels can be accessible for both legitimate users and malicious users. In such environment, there is no guarantee that a route between the two nodes will be free for the malicious users, which will not comply with the employed protocol. The malicious users will attempt to harm the network operations. The primary focus of this work is to provide secure data transmission between the mobile nodes. Rest of the paper is organized as follows. Some of the existing models are presented in section 2.
Section3 presents the proposed model and its functions. Simulation of proposed model is discussed in section 4. Results of this model are presented in section 5. Finally, section 6 presents
the conclusions and future work.

II. EXISTING WORK

The secure routing algorithms in wireless communication are addressed and have been suggested for increasing the security levels[4]. However, these algorithms are unable to protect the network from attackers, who acquired the key information[5]. *J.Li et al*[6] proposed a common key encryption mechanism for MANETs using Dynamic Source Routing(DSR). Drawback of this model is that it dropped more packets even if the network had few malicious users[7]. Adhoc On-Demand Distance Vector(AODV), which is used to provide secure and reliable data transmission over the

MANETs[8]. Several strategies are used to detect the non-cooperate nodes while forwarding the data packets to the destination[9]. In[10], authors discussed a trusted approach to establish the communication between the mobile users. Here, the communication takes place based on the watch dog. The trusted values are represented
from -1 to +1.

A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination[11]. Smith *et al*[12] examined the routing security of distance vector protocols in general and developed countermeasures for vulnerabilities by protecting both routing messages and routing updates. They propose sequence numbers and digital signatures for routing messages and updates as well as including predecessor information in routing updates.

III. PROPOSED MODEL

This model presents a secure communication between the mobile nodes. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node via the cluster head. The authentication service uses a key management to retrieve the public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source. After execution of the key management module, a session key is invoked, this is used by both source and destination for further communication confidentially. In this way, all the important messages are transmitted to the destination.

A. Routing protocol

The paths are maintained as long as source needs. Here, we use sequence numbers to maintain the up-to-date information. The routing information has been updated using Route Request RREQ packet. If the source wishes to communicate with destination, for which it does not have a path, then it broadcast the RREQ packet to the network. After receiving, the intermediate node will broadcast a Route Reply(RRE) packet. If the RREQ packet has already processed, then it will be discard. The proposed model uses Zone Routing Protocol(ZRP). Here, each node proactively maintains a set of possible routes within the region. Knowledge of each region is learned by the ZRP to improve the network performance efficiency. The DSDV is used to learn about nodes within the region. In order to find the routes for nodes, which are out-of-region and DSR is used.

IV. SIMULATION

This model has considered an area of 1000mX1000m with a set of mobile nodes placed randomly and broadcast range is 150m. The simulation was carried out for different number of nodes using Network Simulator (NS2). The node mobility is simulated with a velocity of -20m/s. It sends 30000CBR packets approximately and the simulation parameters are shown in Table I. The performance metrics are packet-delivery ratio, throughput and control message packet.

Table 1. Simulation parameters

Simulation time	2000s
Topology size	1000mX1000m
No. of nodes	1000
No.of clusters	10
No.of cluter heads	10
No. of malicious nodes	7
Node mobility	0 to 10m/s
Transmission range	250m
Routing protocol	ZRP
Frequency	2.4Ghz
Channel capacity	2Mbps
Traffic type	CBR
CBR packet size	512 bytes
Number of packets	30000
Simulator	NS2
Communication system	IEEE802.11g
Pause time	1s
Mobility model	Random way

V. SIMULATION RESULTS

Here, we consider 250 mobile nodes(5 malicious nodes) and 3 cluster heads, number of data packets sends between 5-20 packets/s, and each node moves with 8 m/s. We have executed our model with different arrival of rates of packets for 20times. The simulation results are shown in Figure 2. From the results, we conclude that AODV protocol is delivered around 72% of the packets, while proposed model delivers 60%. For 5 malicious nodes, the proposed model delivers 51% of the packets due to packet loss caused, during the detection phase, i.e., after a malicious node has launched attacker yet before it is finally isolated, whereas AODV and DSR protocols have transmitted with 40% and 35% of the packets respectively.

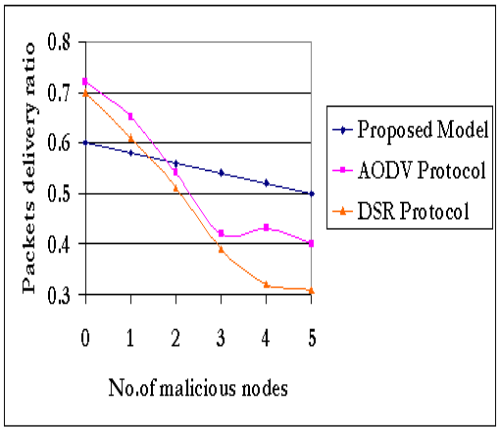

Fig.2. No. of malicious nodes versus packets deliver ratio

Figure 3 shows the number of data packets dropped by the malicious nodes, as total number of data packets is transmitted by the source. Here, we have considered 125 nodes(5 malicious nodes), 2 cluster heads, and number of packets sends between 0-80 packets/s and each node moves constantly with 2 m/s. In DSR model, 47% of the packets are caused by the malicious nodes, while AODV protocol has caused with 39% and the proposed model with 19% of the packets.

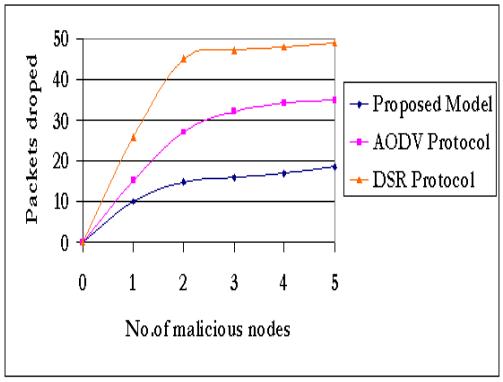

Fig.3. Number of malicious nodes against packet dropped

Network load versus end-to-end delay has shown in Figure 4. Here, we have considered 350 mobile nodes (5 malicious nodes), 4 cluster heads, and number of packets sends between 100-150 packets/s and each node moves constantly with 2 m/s. Initially, all the three models have delivered the data packets with equal delay as long as load is low. If the load increases, then the end-to-end delay of the packet is increased. From the results, we conclude that AODV has delivered the data packets at low delay as compared to other protocols.

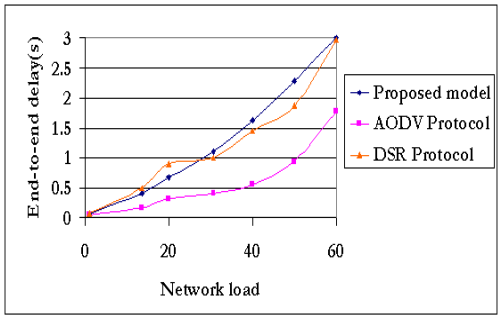

Fig.4. Network load against end-to-end delay.

VI. CONCLUSIONS AND FURTHER RESEARCH WORK

There are various MANET protocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes. It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks. In this model, we have discussed the security issues for MANETs. It focuses on the security architecture. Since, every attack has own characteristics. One of the limitations of this model is that it works based on the assumption of malicious nodes, which do not work as a group. It may be happened in a real situation.

REFERENCES

[1] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L.Zhang, "Security in Mobile Adhoc Networks: Challenges and Solutions", *IEEE Wireless Communications*, Vol. 11, pp. 38-47(2004).

[2] A. Perrig et al., "The TESLA Broadcast Authentication Protocol", *RSA Crypto Bytes*, Vol. 5, No. 2, p. 2-3(2002).

[3] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Adhoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 2, No. 3, pp. 257-269(2003).

[4] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", *ACM Wireless Networks*, Vol. 9, pp. 545 – 556(2003).

[5] Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Adhoc Routing," IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 28- 39(2004).

[6] J. Li, J. Jannotti, Douglas S. J. D. Couto, David. R. Karger, and R. Morris, "A Scalable Location Service for Geographic Adhoc Routing", *In Proceedings of International Conference on Mobile Computing and Networking*, pp. 120-130(2002).

[7] B. Karp and H. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", *In Proceedings of International Conference on Mobile Computing and Networking*, pp. 243- 254(2003).

[8] Y. A. Huang and W. Lee, "Attack Analysis and Detection for Adhoc Routing Protocols," *In Proceedings of* International *Symposium on Recent Advances in Intrusion Detection*, pp. 125-145(2004).

[9] L. Zhou S. B. Fred, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority", *ACM Trans. On Computer Systems*, Vol. 20, No. 4, pp. 329- 368(2002).

[10] M. Gasser and E. McDermott, "An Architecture for Practical Delegation in a Distributed System", *In Proceedings of IEEE Symposium on Security and Privacy*, pp. 20- 30(2004).

[11] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of Zone Routing Protocol", *IEEE Trans. on Networking*, vol. 9, no. 4, pp. 427-438(2001).

[12] Bradley R. Smith, Shree Murthy, and J.J. Garcia-Luna-Aceves, "Securing Distance- Vector Routing Protocols", *In Proceedings of Internet Society Symposium on Network and Distributed System Security*, pp. 85-92(1997).