Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Detection and avoidance of node misbehavior in MANET based on CLAODV

S.Usha[1] and S. Radha[2]

[1]*Sathyabama University, Chennai -600119, India*
[2]*ECE Department SSN College of Engineering, Chennai- 603110, India*
usha_sakthivel@yahoo.co.in; radha_kumaran@yahoo.co.in

Abstract

This paper depicts a model which not only evaluates the node's reputation, but also avoids the malicious node in the forwarding path. The simulation is performed by using the NS2 software. This model uses the IEEE 802.11 protocol with RTS, CTS, DATA and ACK signalling at the MAC layer. The paper models packet forwarding, passive misbehavior, active misbehavior and avoidance of malicious nodes in the route. The model also takes into account the blocking caused by the hidden node problem in wireless networks. The results achieved are both graphical as well as in the form of a network animation. Curves such as throughput and jitter are plotted to analyse the performance of the MANET.

Keywords*:* RTS, CTS,Clone Node, Jitter , Throughput

Introduction

Network security is a challenging aspect in Mobile Ad hoc Networks (MANETS). The MANETs suffer from various attacks and threats such as misbehavior and clone nodes. Moreover, attacks occur across multiple layers, these days. This paper models and studies the impact of misbehavior (active and passive) and clone nodes and also proposes a solution to avoid the potential malicious nodes. The paper also incorporates a cross layer approach to the AODV protocol. This is done by adding additional parameters such as Receiver threshold, CP threshold and CS threshold to the existing AODV to formulate a CLAODV (Cross Layer AODV). The impact of the devised model on throughput and delay are also studied.

Present system

The present systems are designed exclusively to only monitor the behavior of nodes, i.e., whether a node is well behaved or misbehaving (Mian et al., 2009). The watchdog model (Marti et al., 2000), which is currently employed works only at the network layer and hence faces problems such as the case of a monitored collision (Abderrezak Rachedi, 2007) and interference due to hidden terminal problem(Ververidis & Polyzos, 2008). For dealing with cloned nodes, the simple RSA algorithm is not very secure owing to its deterministic nature.

The cross layer AODV does not need any major modification in original AODV. Handling of RREP and RERR packets (Wang & Garcia-Luna-Aceves, 2002), of basic AODV are left as they are. And no other function of routing layer including communicating with the MAC and network layers is changed The CLAODV results in improved packet delivery ratio and average end to end delay performance in heterogeneous networks, which are most important for best effort traffic.

Proposed system

In the proposed work, first the scenario of misbehaving node is created and its impact on the MANET is studied. Second, clone nodes are modelled and an adaptive RSA is used to avoid such clone nodes. Finally, a CLAODV approach combined with adaptive RSA is used to combat all forms of malicious nodes. The graphs of throughput versus load and delay versus time are plotted.

Description

Module design

Passive misbehavior and packet forwarding: The module performs the functions such as: Creates a MANET, Routes packet from source node to destination node using AODV and Models passive misbehavior.

Active misbehavior- forwarding to wrong destination: The function of the module includes: Creates the MANET and Models four malicious nodes which alter the destination IP of the packet to forward it to the wrong destination.

Active misbehavior- Looping: The module performs functions such as: creates the MANET and models four malicious nodes which alter the destination IP of the packet to forward it to the source itself.

Active misbehavior- Intentional dropping: The functions of the module are: Creates the MANET and models four malicious nodes which simply drop the packets after they receive.

Clone node-Single hop MANET: It creates a single hop MANET, models three clone nodes and uses adaptive RSA to avoid the clone nodes.

Clone node-Multi hop MANET: It creates a multi hop MANET, models three clone nodes and uses adaptive RSA to avoid the clone nodes.

Avoidance and isolation of misbehaving nodes: Uses CLAODV to improve performance of MANET, uses adaptive RSA to avoid clone node attack and uses Cross layer monitoring and avoidance of malicious nodes.

Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig.1. Network Initialization-stage 1

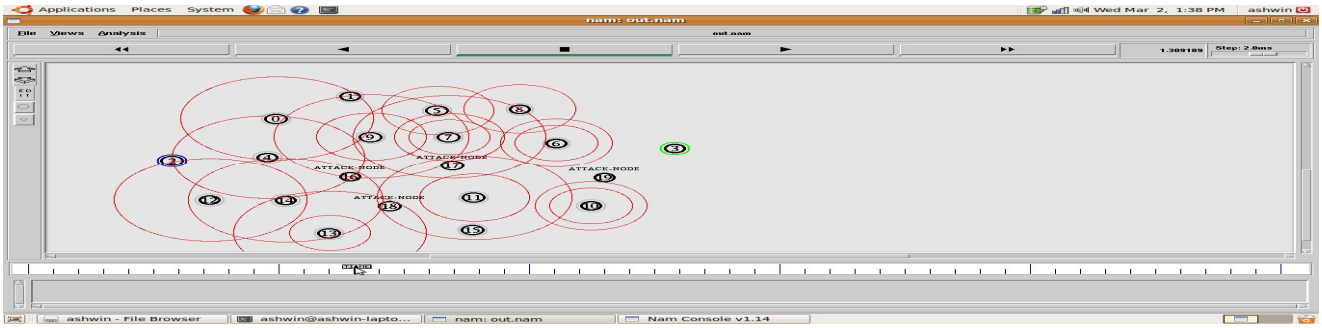


Fig. 2. Network initialization-stage 2

Fig. 3. Packet forwarding from source to node

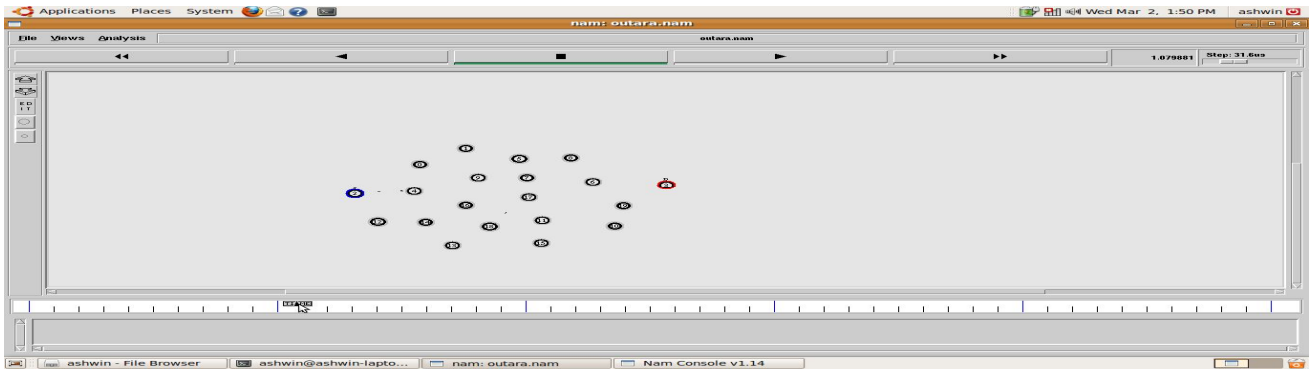
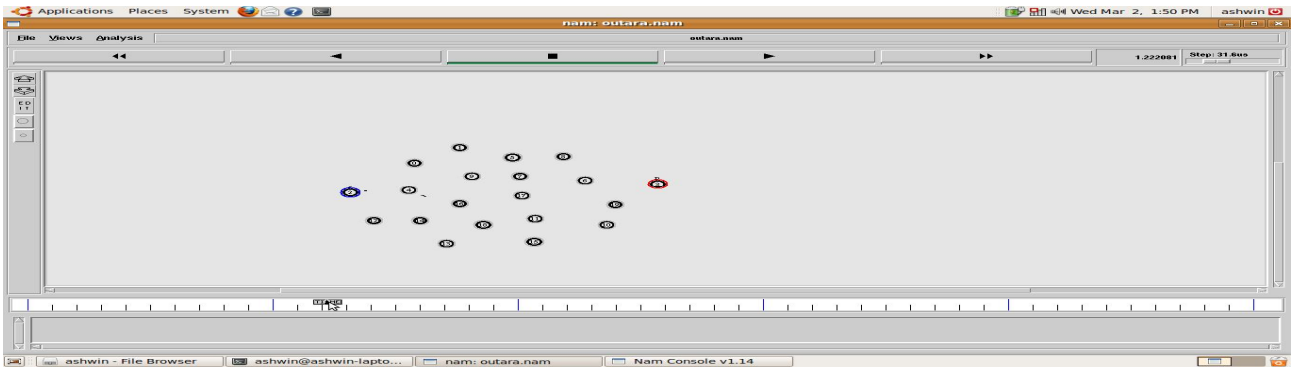


Fig. 4. Packet forwarding from node 4 to node 16



Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig. 5. Packet forwarding from node 16 to node 11

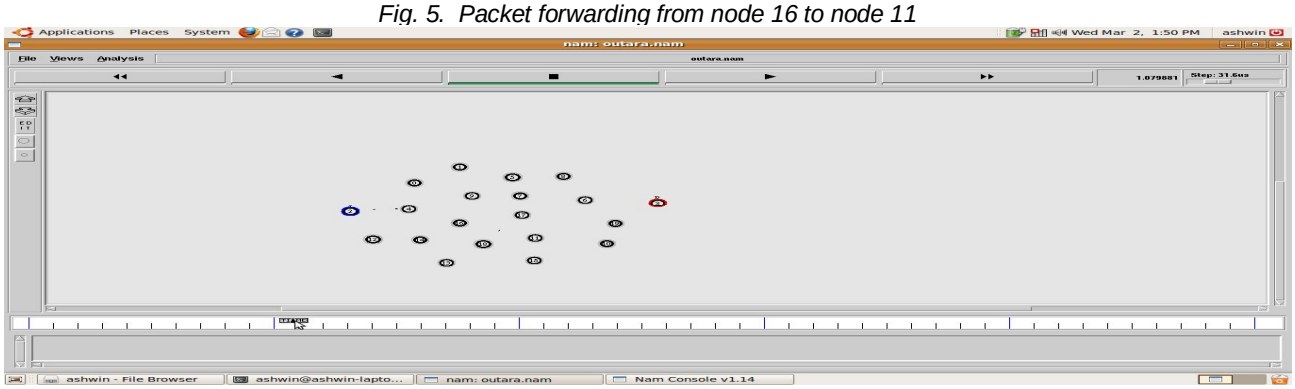


Fig. 6. Packet forwarding from node 11 to node 6

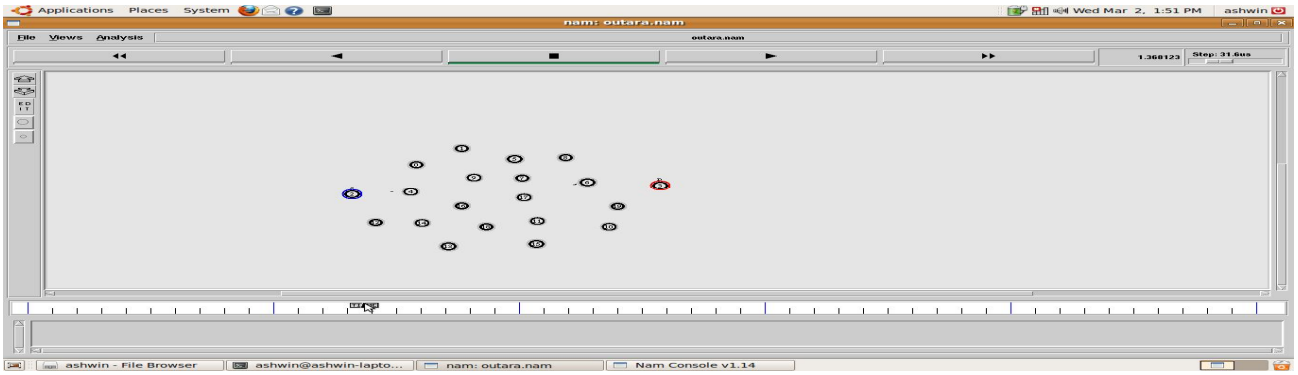


Fig. 7. Packet forwarding from node 6 to destination

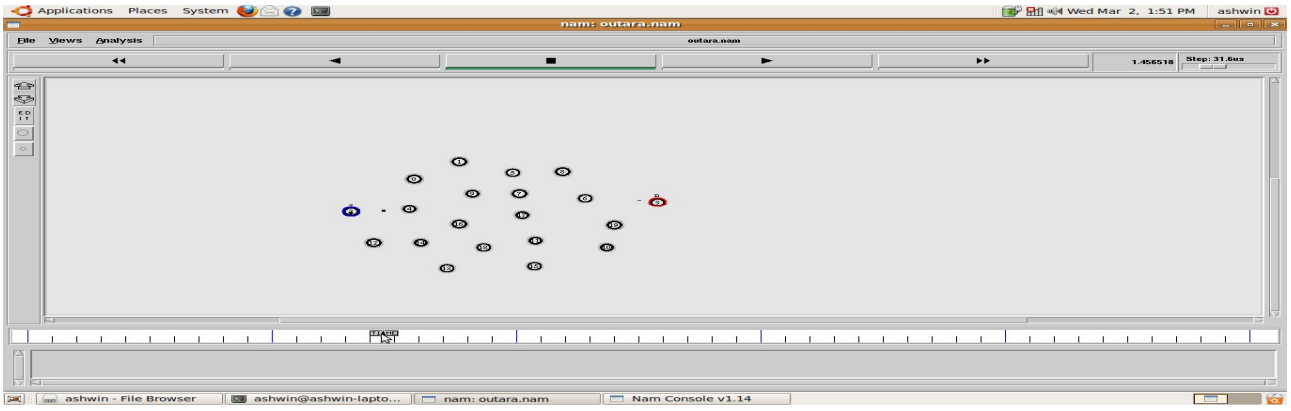
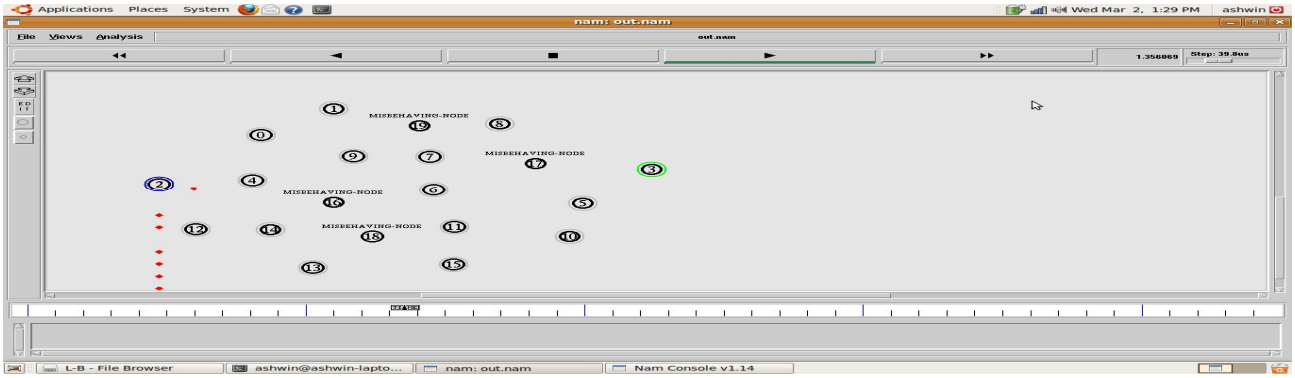


Fig. 8. Passive Misbehavior



Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig. 9. Active Misbehavior- Intentional packet dropping

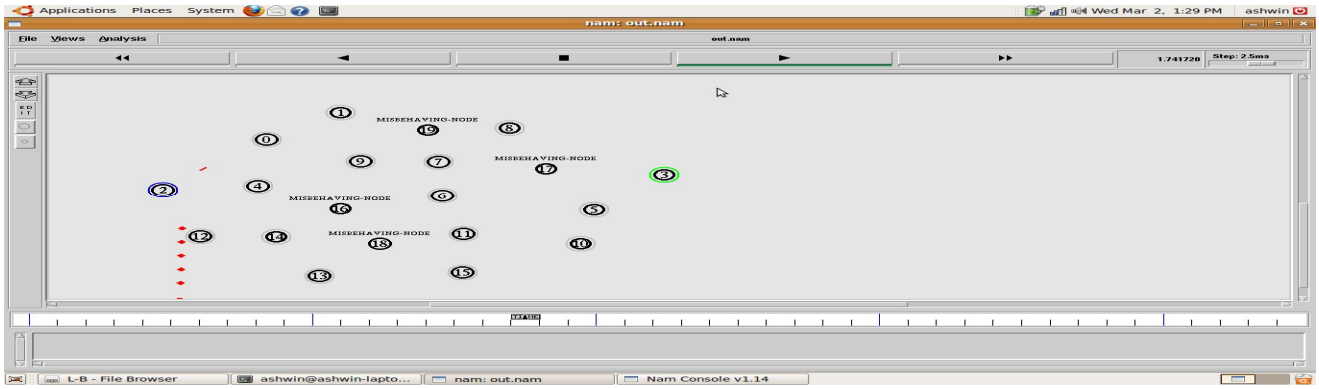


Fig. 10. Active Misbehavior-Looping of packets -snapshot 1

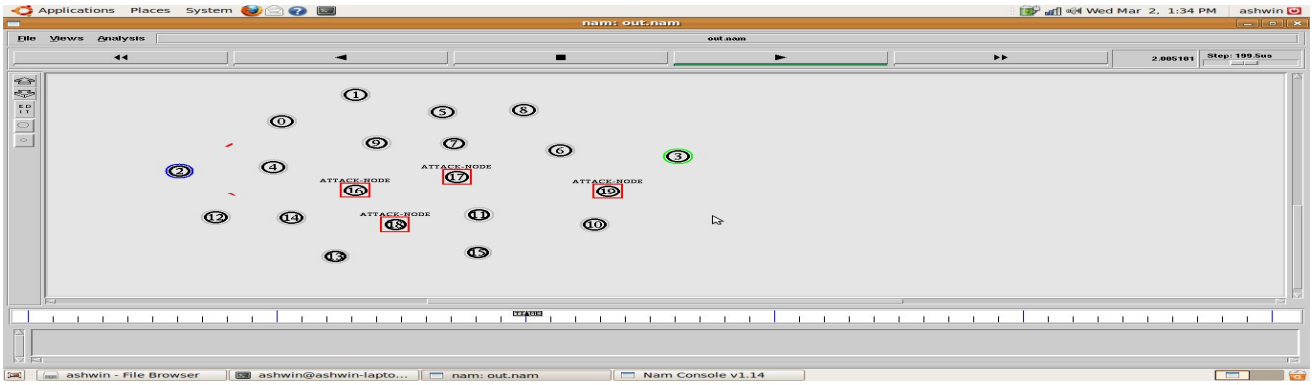


Fig. 11. Active Misbehavior-Looping of packets - snapshot 2

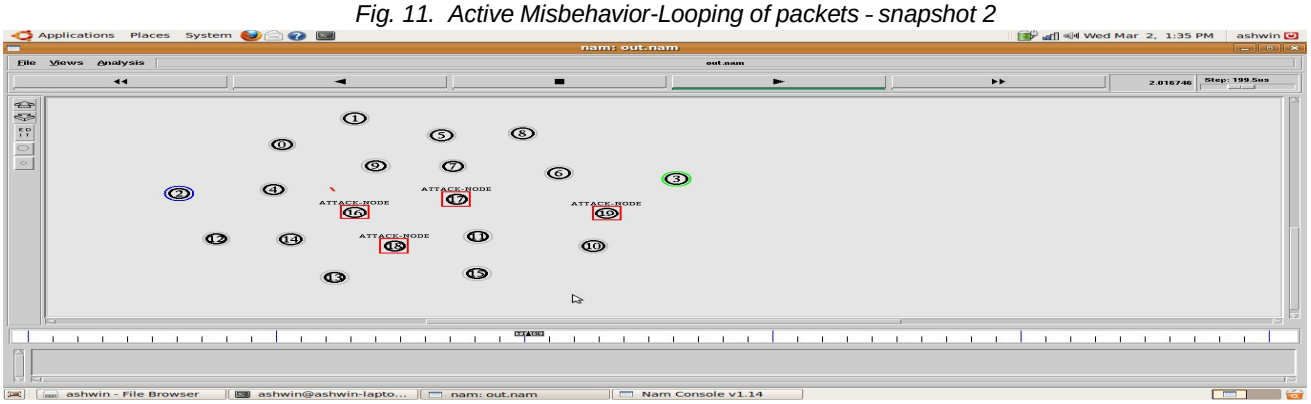
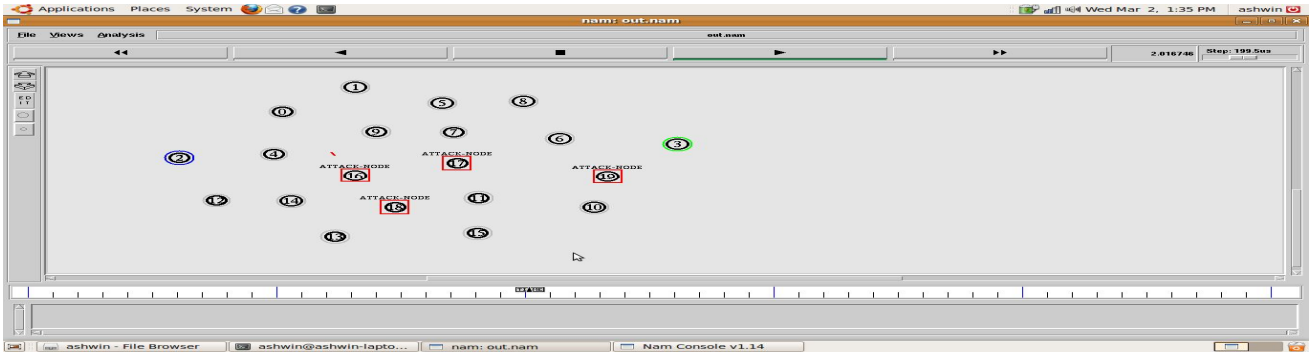


Fig. 12. Active Misbehavior-Looping of packets - Snapshot 3



Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig. 13. Active Misbehavior-Forwarding to wrong destination (Node 2 is source and node 3 is destination)

Fig. 14. Active Misbehavior-Forwarding to wrong destination (Node 2 is source and node 3 is destination) Packet if forwarded to node 10, the wrong destination

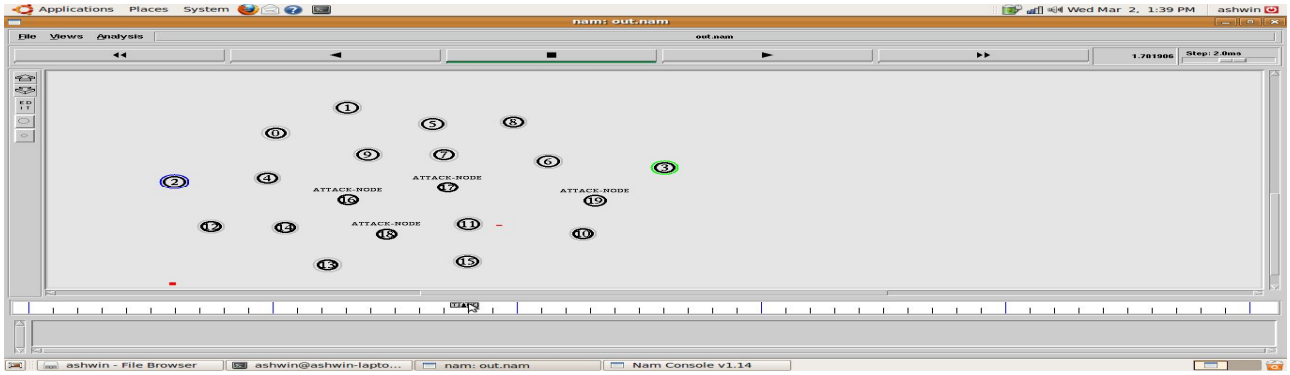


Fig. 15. Active Misbehavior-Forwarding to wrong destination- Misbehavior introduced by node 10

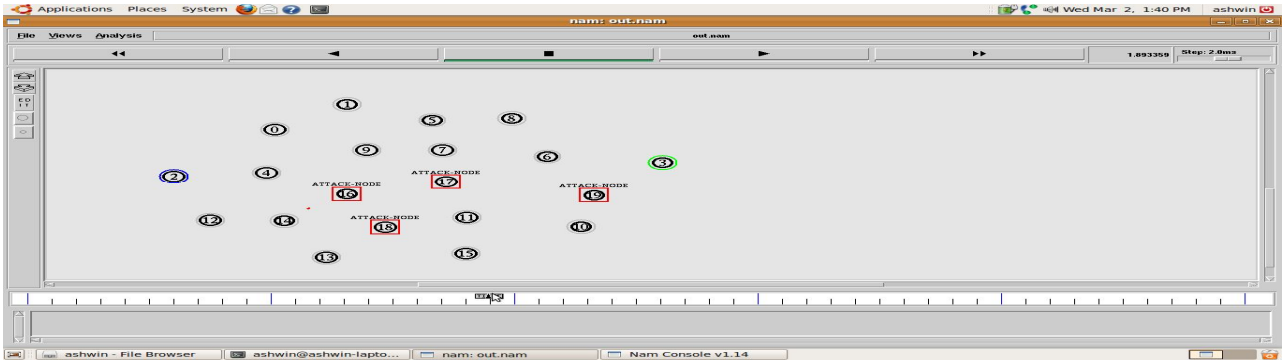
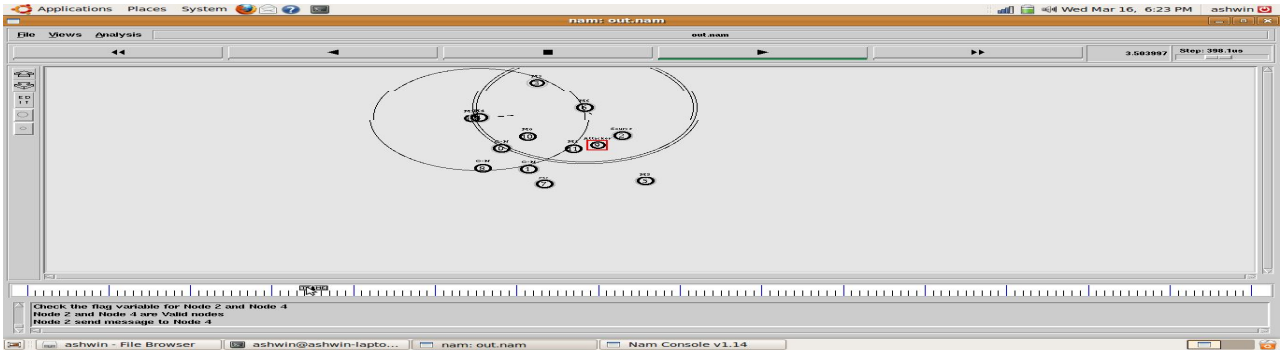


Fig. 16. Cloned node attack



Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig. 17. Misbehavior detection and avoidance

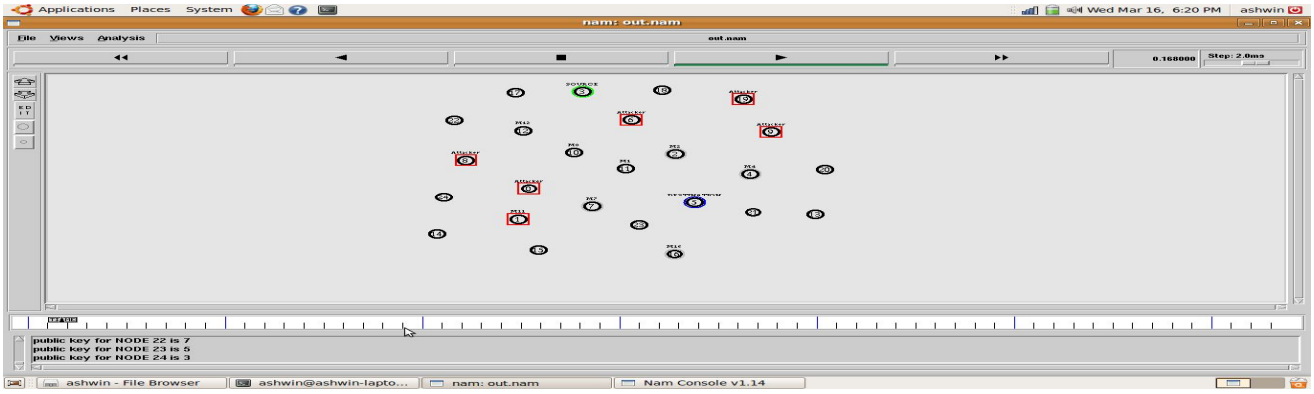


Fig. 18. Misbehavior detection and avoidance- Packets sent from source to node 10 avoiding the misbehaving nodes

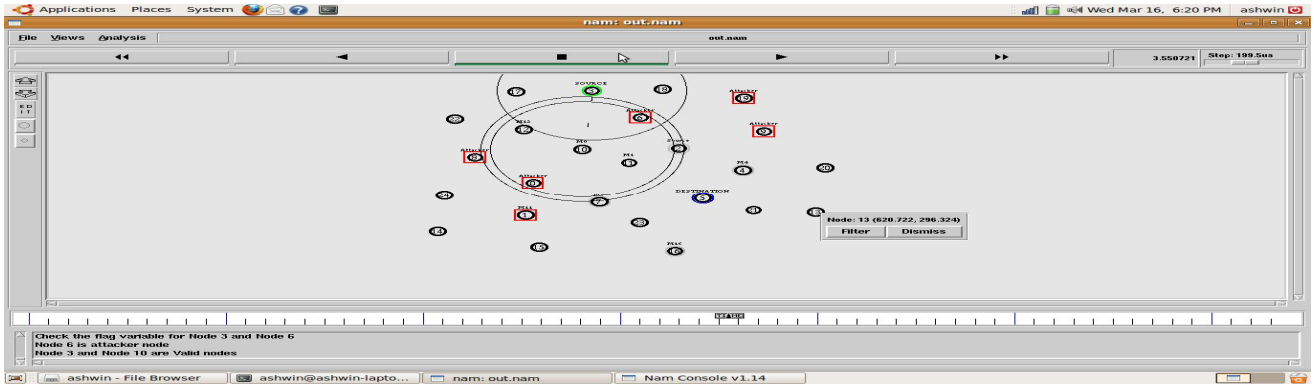


Fig. 19. Misbehavior detection and avoidance- Packets sent from node 10 to node 11 avoiding the misbehaving nodes

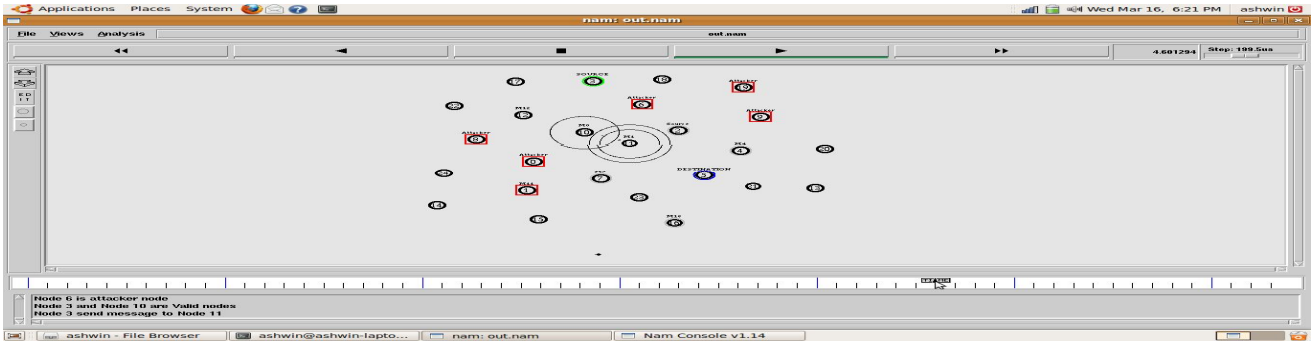
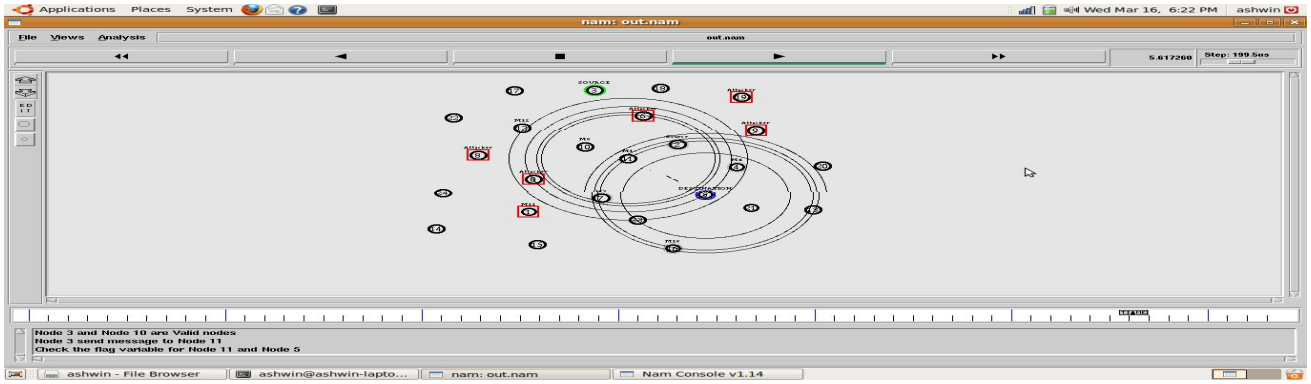
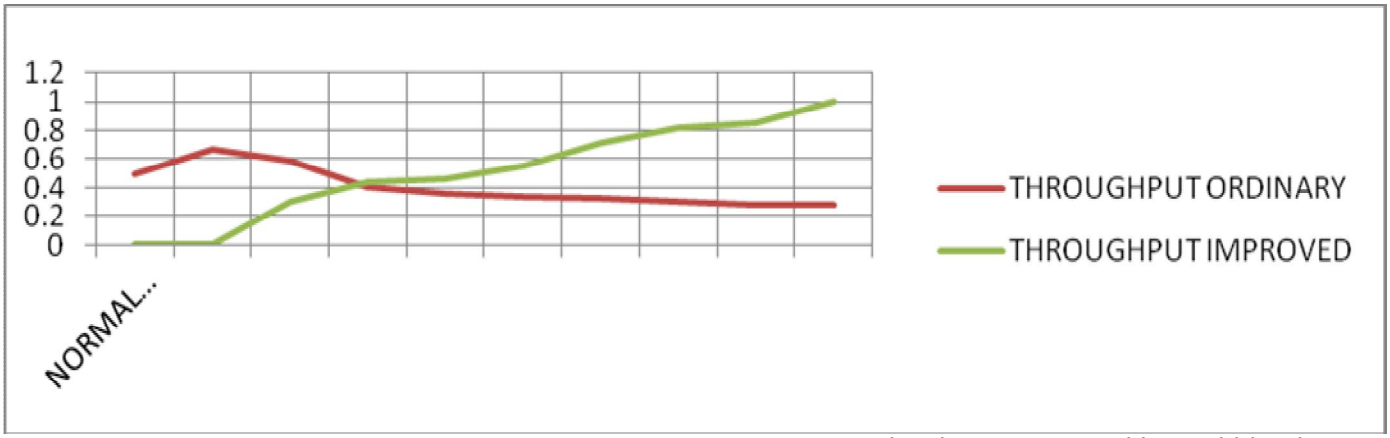


Fig. 20. Misbehavior detection and avoidance- Packets sent from 11 to destination Avoiding the misbehaving nodes



Indian Journal of Science and Technology Vol. 4 No. 10 (Oct 2011) ISSN: 0974- 6846

Fig. 21. Performance curves



Specifications of layers

The physical layer specifications encompasses Antenna-Omni directional; Propagation mode (Xu et al., 2003), l-Two ray ground theory; Topology-Two degrees of freedom (1500x1500); Channel-Wireless with random noise; Mobility model-Random; Service category-CBR; Transmit power: 0.281838; Frequency: 9.14e+08; Transmit antenna height: 1.5; Receive antenna height: 1.5; Receiving threshold RXThresh_ is: 3.65262e-10and P.s. $(0.28183815\times1.5^2\times1.5^2) / (250^4)=3.652e-10$.

The MAC layer specifications include Protocol-IEEE 802.11 with RTS, CTS, DATA and ACK signalling; Queue-Drop tail & Priority queue; Queue size-As per requirement (Dipanjan *et al*., 2006); Time duration-5 units for simulation and Max no. of retransmissions-3 (defined in NS-2).

The Network layer specifications comprise Routing protocol-AODV; Agents like UDP, Loss monitor agent, Null agent and Custom defined agent for trace.

Implementation and results

The implementation and results are presented in Fig.1 to 21

Fig.21 explains the cross layer design involving CLAODV; adaptive RSA at the application layer improves the throughput of the MANET dramatically at high loads. The reason for low throughputs at low loads is attributed to the overheads generated by the control signalling. Though the initial delay is higher, the delay subsequently drops to a normal value at the same time become robust to all forms of attacks and maliciousness. For normalized load less than 0.6, the performance of ordinary MANET is superior.

Conclusion and future prospects

At higher loads, the MANET that incorporates CLAODV and adaptive RSA is superior. The throughput achieved is more than double that achieved in an ordinary MANET. Thus, the project will help a reliable and secure MANET whose performance is superior to the existing system. The current system works using the 802.11b MAC protocol. Advancement to this would be the use of frequency hop spread spectrum 802.11a in addition to the existing transmission mechanism which aids to reduce issues like near-far terminal problem. The approach can also be extended to infrastructure networks to provide secure radio communication.

References

1. Abderrezak Rachedi (2007) Cross-Layer approach to improve the monitoring process for mobile ad hoc networks based on IEEE 802.11. IEEE Globecom Proc. pp: 1086-1091.
2. Dipanjan Anupam J, Yelena Y and Tim F (2006) Toward distributed service discovery in pervasive computing environments. *IEEE Trans. Mobile Computing*. 5 (2), 97-112.
3. Marti S, Giuli TJ, Lai K and Baker M (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proc. of the 6th Annual ACM/IEEE Intl. Conf. on Mobile Computing & Networking. pp: 255-265.
4. Mian AN, Baldoni R and Beraldi R (2009) A survey of service discovery protocols in multihop mobile ad hoc networks. *IEEE Pervasive Computing*. 8 (1), 66-74.
5. Shakkottai S, Rappaport TS and Karlsson PC (2003) Wireless networks. IEEE Commun. Mag. 41, 74-80.
6. Ververidis CN and Polyzos GC (2008) Service discovery for mobile ad hoc networks: a survey of issues and techniques. *IEEE Commun. Surveys &Tutorials*. 10(3), 30-45.
7. Wang Y and Garcia-Luna-Aceves JJ (2002) Performance of collision avoidance protocols in single-channel ad hoc networks. In: Proc. of IEEE ICNP.
8. Xu K, Gerla M and Bae S (2003) Effectiveness of RTS/CTS Handshake in IEEE 802.11 based ad hoc networks. Ad Hoc Network.pp: 98-106.