ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

DETECTION OF CLONE MISBEHAVIOR USING CROSS LAYER AODV

M.Savithri[1], P.Dharani selvi[2]

Assistant professor, Department of Computer science, Dr.N.G.P Arts and Science College, Coimbatore, India[1]

M.phil Research Scholar, Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore, India[2]

Abstract: Wireless Ad-hoc network particularly Mobile Ad-hoc Networks are highly vulnerable to intrusion, node compromise and physical capture attacks can easily destroy the network, since they are not protected by any high resistant hardware due to their low-cost and small size. If they are captured the devices can be easily compromised and cloned. The cloned devices will have the same identity as legitimate devices and interact with other devices in the network. This paper depicts a model to evaluate the node's reputation, and also avoids the malicious node in the forwarding path. This model uses the IEEE 802.11 protocol
with RTS, CTS, DATA and ACK signaling at the MAC layer. This paper models packet forwarding, passive misbehavior, active misbehavior and avoidance of malicious nodes in the route. Curve such as throughput and jitter are plotted to analyse the performance of the MANET.

Keywords: Throughput, MANET, Jitter, Clone nodes

I. INTRODUCTION

Network security is a challenging aspect in Mobile Ad hoc network (MANETs). The MANETs suffer from various attacks and threads such as misbehavior and clone nodes, these days. This paper models and studies the impact of misbehavior of clone nodes using Cross Layer AODV Protocol. This is done by adding additional parameters to the existing AODV to formulate a CLAODV. The result of CLAODV is improved packet delivery ratio and throughput

II. BRIEF DESCRIPTION OF AODV

To understand the details of our scheme a brief description of AODV is provided. In AODV routing, whenever a route from a source to a destination need to be found, the route discovery process is initiated by broadcasting route request from the source and propagate through the entire network. When the destination or a intermediate node with route to the destination receive the route request, it sends the back a reply to the initiator of the route request. These control message are send during the route discovery phase, are responsible for updating the route table of the source, destination and all the intermediate nodes. They are used by the routing protocols to route the packets. However, we primarily focus on the strategies to minimize the effects of attacks against these protocols.

A. Route discovery

To perform a route discovery, the source node broadcast a route request packet with a recorded source route listing by itself. Each node that hears the route, forwards the request (if appropriate), adding its own address to the recorded source in the packet. The route request packet propagate hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target.

B.Route maintenance

If the status of a link or node changes to all other nodes, presumably resulting in the computation of the new route. However, using route discovery, there are no periodic messages of any kind from any of the mobile nodes. Instead, while a route in use, the route maintenance procedure monitors the operation of the route and informs the sender of any routing error. Route maintenance can also be performed using end-to-end acknowledgements rather than the hop-by-hop acknowledgements.

III. CLAODV

The cross layer AODV does not need any major modification in original AODV. Handling of RREP and RERR packets of basic AODV are left as they are. Some additional parameters added to improve the packet delivery ratio and average end to end delay performance in heterogeneous network

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

IV. PROPOSED SYSTEM

In the proposed work, first the misbehaving nodes is created and the impact on the MANET is studies. A CLAODV approach combined with adaptive RSA is used to combat all forms of malicious nodes.

A.Moduledesign

1.Passive misbehavior and packet forwarding: The module performs the function such as creates a Manet route packet from source to destination node using AODV and models passive misbehavior.

2. Active misbehavior- forwarding to wrong destination: The functions of the module include the creation of Manet and four malicious nodes which alter the destination IP of the packets to forward it to the wrong destination.

3. Active misbehavior- looping: The module performs function such as creates the Manet and models four malicious nodes which alters the destination IP of the packets to forward it to the source itself.

4. 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.

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

6. Clone node- multi hop Manet: it creates a multi hop Manet, models three clone nodes and uses adaptive RSA to avoid the clone nodes.

7. Avoidance and isolation of misbehaving nodes: Uses CLAODV to improve performance of Manet, uses adaptive RSA to avoid clone nodes attacks and uses cross layer monitoring and avoid the malicious nodes.

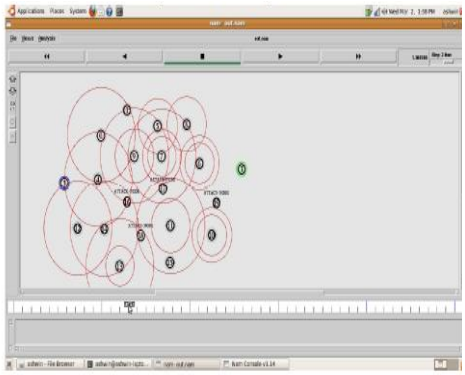

Fig 1.Network Initialization stage 1

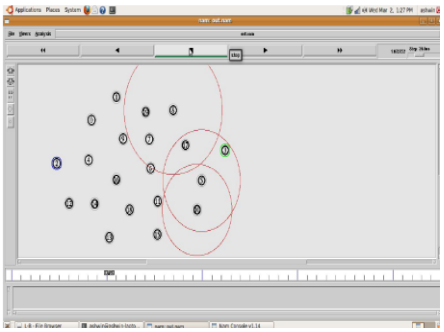

Fig2. Network Initialization stage 2

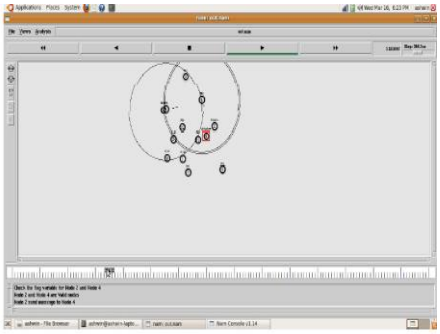

Fig 3:Cloned node attack

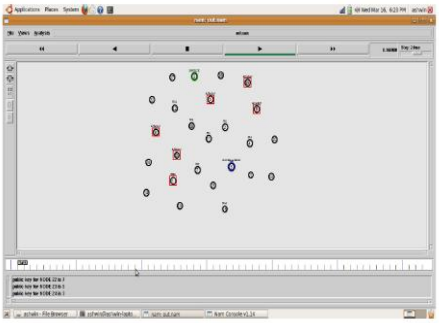

Fig4: Avoidance and Isolation of Clone Nodes

Fig 5Throughput Increased Using CLAODV.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

V SPECIFICATION OF LAYERS

The MAC layer specifications include Protocol-IEEE 802.11 with RTS, CTS, DATA and ACK signaling Queue-Drop tail & Priority queue; Queue size-As per Requirement, Time duration-5 units for simulation and Max no. of retransmissions-3. The Network layer specifications comprise Routing protocol-AODV; Agents like UDP, Loss monitor agent, Null agent and Custom defined agent for trace. 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 signaling. 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.

V. CONCLUSION

At a higher load the MANET that incorporates CLAODV is superior. The throughput achieved using the Cross Layer AODV is comparatively high than in the ordinary MANET. Thus the project will help in reliable and secure MANET routing and whose performance is superior to the existing system. Advancement to this would be using frequency hop spectrum 802.11a in addition to the existing transmission mechanism which avoids to reduce issues like near-far terminal problem. This approach can be also extended to infrastructure network to provide secure radio communication.

REFERENCES

[1] Johnson D.B. and Maltz D.A., Broch J.,(1996),"The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-hoc Networks,"Mobile Computing", pp 153-186.

[2] Yin L. and Cao G.," Supporting Cooperative Caching in Ad Hoc Networks," Dept of C.S.E,The Pennsylvania State University, University Park, 16802.

[3] He Y. and Berson S., "Active Packets Improve Dynamic Source Routing for AD Hoc Networks," Deptt of Computer Science University of Southern California, Information Sciences Institute University of SouthernCalifornia,2010.

[4] Shanmugavadivu K. and Madheswaran.**"**Caching Technique for Improving ata Retrieval Performance in Mobile Ad Hoc Networks**,"**K.S. Rangasamy College of Technology/Tiruchengode-637215.2009

[5] K.R.S. and Rajanikanth K. **"**Intelligent Caching in on-demand Routing Protocol for Mobile Ad Hoc Networks**",**2009

[6] Rawa A., et al **, "**Enhanced DSR for MANET with Improved Secured Route,discovery and QoS," Department of Electronics and Telecommunication Engineering, Shri G. S.Institute of Technology and Science, India School of Computer Science, DAVV, Khandwa Road Campus, India.,2007

[7] Wang Y and Garcia-Luna-Aceves JJ ,Performance of collision avoidance protocols in single-channel ad hoc networks. In: Proc. of IEEE ICNP.2002

[8] Xu K, Gerla M and Bae Effectiveness of RTS/CTS Handshake in IEEE 802.11 based ad hoc networks. Ad Hoc Network.pp: 98-106.2003

[9] Abderrezak Rachedi Cross-Layer approach to improve the monitoring process for mobile ad hoc networks based on IEEE 802.11. IEEE GlobecomProc. pp: 1086-1091,2007