ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Trapdoor Exposure using Markov Model

Rajni Bhatnagar[1], Jitendra Arora[*2]

[#]*Department of cse, DeenBandhu Chotu Ram University*

Abstract: Mobile network is one of most common ad hoc network with problems related to congestion and routing. Trapdoor exposure disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network and may severely damages the communication among the nodes. We are providing one of the solutions to secure the transmission over the network as security aspects play an important role in almost all of the application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that mobile communication takes place to routing, man-in-the-middle and elaborate data injection attacks. To resolve the problem of trapdoor exposure we are using cryptographic handshaking along with HMM. The presented approach will improve the network throughput effectively.

Key Terms: - Mobile ad hoc network; Trapdoor exposure; routing protocols; Markov Model,Handshaking

INTRODUCTION

Ad hoc is used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a wireless base station to a network in which connection established for a single session and does not require a router For example, if you need to transfer a file to your friend's laptop, you might create an ad- hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a multi-hop ad hoc network, which can transfer data over multiple nodes.

Trapdoor exposure is non cooperation in certain network operations, i.e. dropping of packets which may affect the performance, but can save the battery power. The proposed work is about to identify the Trapdoor nodes and perform the communication over an effective node from the network. It will improve the network throughput. Along with this the work will give an efficient and reliable transmission over the network. In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members[7]. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by AODV to ensure the

freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes

CONCLUSION

The proposed work is about the prevention of Trapdoor exposure. The proposed system is based on HMM based parametric analysis while performing the next node selection. The HMM parameters taken here are the loss rate, transmission rate and the network delay. The HMM on these all parameters is performed to identify the critical node as well as the safe node. On each node, the HMM rule is implemented to identify the safe path. The process is repeated on each node till the destination is not achieved. The system is providing better throughput and less packet loss over the network. The system is implemented in a wireless network with AODV protocol. In this system a neighbor node analysis is performed under different parameters to provide the network security in case of Trapdoor exposure. Here we have proposed a new algorithm for the above said task. The implementation is performed in ns2 and analysis is presented using x graph.

ACKNOWLEDGMENT

Assistant Prof. Jitendra Arora is the assistant professor in Department of Computer Science and Engineering at Royal Institutes of Technology and Management, Chidana, Haryana. I am especially grateful for his guidance and contributions by generously giving his time and carefully reviewing this manuscript.

REFERENCES

[1]Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", 978-1-61284-486-2/111 2011 IEEE

[2] Jong-Pyng Li," Priority Based Real-Time Communication for Large Scale Wormhole Networks", 0-8186-5602-6/*9*04 1994 IEEE

[3] Junfeng Wu," Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE

[4] L. Lazos," Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", IEEE Communications Society / WCNC 2005 0-7803-8966-2/05 © 2005 IEEE

[5] Lixin Tao," AN ON-LINE SIMULATOR FOR WORMHOLE ROUTING NETWORKS".

[6] Luis Gravano," Adaptive Deadlock-free Worm-hole Routing in ypercubes.", 0-8186-2672-0/92 @ 1992 IEEE

[7] Majid Khabbazian," Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 1536-1276/09@ 2009 IEEE

[8] Manolis G. H. Katevenis," Wormhole IP Over (Connectionless) ATM", IEEE/ACM TRANSACTIONS ON NETWORKING 1063–6692/01© 2001 IEEE

[9] Mariannne. A. Azer, "Wormhole Attacks Mitigation", 2011 Sixth International Conference on Availability, Reliability and Security

[10] Pallavi Sharma Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 978-1-61284-486-2 IEEE

[11] Ronald I. Greenberg," Universal Wormhole Routing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 1045-9219/97©1997 IEEE

[12] Sanjay Keer," To Prevent Wormhole Attacks Using Wireless Protocol in MANET", Int'l Conf. on Computer & Communication Technology 978-1-4244-9034-/10©2010 IEEE

[13] Sami Taktak," A Polynomial Algorithm to Prove Deadlock-Freeness of Wormhole Networks", 2010 18th Euromicro Conference on Parallel, Distributed and Network-based Processing 1066-6192/10© 2010 IEEE

[14] Saurabh Gupta Subrat Kar S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", 2011 International Conference on Innovations in Information Technology

[15] Sergio Felperin," A Theory of Wormhole Routing in Parallel Computers", 0-8186-2900-2/92@1992IEEE

[16] Viren Mahajan," ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS", 978- 1-4244-2677-5/08©2008 IEEE

[17] Xiaola Lin," Deadlock-Free Multicast Wormhole Routing in 2-D Mesh Multicomputers", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 1045-92 I9/94@ I994 IEEE

[18] Yih-Chun Hu," Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", 0-7803-7753-2/03© 2003 IEEE

[19] Yih-Chun Hu, "Wormhole Attacks in Wireless Networks", I EEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[20] Yun Wang," A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE