Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Optimized Scheme for Time-based Cluster Wormhole Detection Protocol

Jagteg Singh[1,]
[1] Research Scholar,
Department of Computer Science,
Global Institute of Management and Emerging Technologies,
Amritsar, India

Er.Prabhdeep Singh[2]
[2]Associate Professor,
Department of Computer Science,
Global Institute of Management and Emerging Technologies,
Amritsar, India

Abstract— Modern communication is containing different types of wireless networks as backbone for various applications used for different users. Mobile Ad-hoc Networks contains many mobile devices and prove to be the good option for communication in various applications including military, industry and remote areas (flood hit areas, nuclear hit areas etc). Generally due to limitations of energy carrying capacity, on demand routing usually vulnerable to various attacks which can be harmful for ad-hoc communication. Wormhole attack is one of the attacks which is very harmful to the ad-hoc communication. Wormhole attack is the most occurring attack in mobile ad-hoc network. This attack is very much active in case of Reactive Protocols such as Ad-hoc On Demand Distance Vector Protocol. In this paper, we have proposed innovative algorithm for prevention of wormhole attack in mobile ad-hoc network. The algorithm successfully isolates the wormhole attack with 50 nodes in wireless communication.

Keywords— Wormhole Attack, AODV, Multipath Algorithm, On Demand Routing Protocols, Route Request, Route Reply, Mobile Ad-hoc Network,

I. INTRODUCTION

In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is the most dangerous and sort of hidden attack. Wormhole attack usually has two attacker nodes which create a tunnel by skipping other nodes and start transfer information to other end of attacker node. Malicious nodes have different range and can be placed on different locations which perform a tunnel of high speed link via a secrete channel. [15] These nodes can act as router or host or both at same time. They can form random topologies depending on their connectivity with each other in the network. [16] These nodes have the ability to arrange themselves and because of their self-configuration ability, they can be deployed immediately without the need of any infrastructure. The major performance constraint comes from path loss and multiple path fading. Many MANET routing protocols exploit multiple paths to route the packets. [17]

II. AODV (AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL)

AODV is an on-demand routing protocol [2]. The AODV algorithm gives an easy way to get change in the link situation. [3] If link failure occurred than notifications are sent only to the affected nodes within range in the network. Generally after receiving this notification, it cancels almost all the routes through this affected node. [7] Generally maintenance of AODV process is based on timely updates which suggest that entries into AODV process expired after timer expires. Further updated information is passed to the neighbors so that it can be updated about route breakage. Discovery of various routes from single source to various destinations is totally based on query and reply packets and intermediate nodes use logs to store the information of routes in route table. Various control messages which are used for the discovery and corrupted routes are as follows: [7] Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR), HELLO Messages. [7]

A. Route Request (RREQ)

Various route request packet are flooded through the network when a route is not available for the destination from source. [3][4][5] Pair source address and request ID identify RREQ and counter is incremented every time source node sends a new RREQ. [5][6] After receiving of request message, each node checks the request ID and source address pair. The new RREQ is discarded if there is already RREQ packet with same pair of parameters. [8] Node with no routes information to particularly destination or any destination will be discarded and information is broadcasted to update information to other routes. [9] A route reply (RREP) message is generated and sent back to source if a node has route with sequence number greater than or equal to that of RREQ.

B. Route Reply (RREP)

On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node. [10]

C. Route Error Message (RERR)

The neighbour-hood nodes are monitored. When a route that is active is lost, the neighbour-hood nodes are notified by route error message (RERR) on both sides of link. [6].

III. WORMHOLE ATTACK

Wormhole attack is always launched by attacker who tunnels packets at one point to another point in the network, and then use to reply to the sender again. The wormhole attack can have dangerous effects threat in mobile ad-hoc networks, especially against many On Demand protocols for ad hoc network routing protocols. [14]

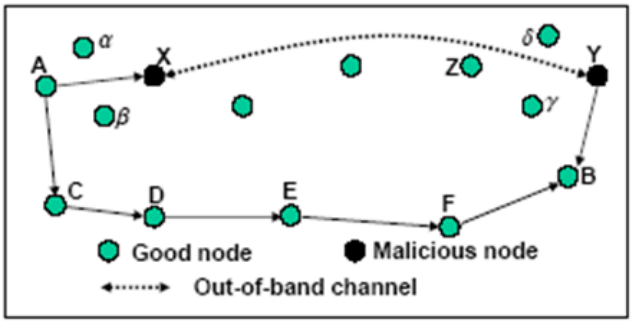

Figure 1: Wormhole attack demonstration

It is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. [6] [7] [8] During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. [9] [10] [11] Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand). [12]

IV. PROBLEM DEFINITION

The idea behind using the k-means cluster analysis to detect wormhole attack relies on the distance correlation in the physical locations of nodes. According to the ToA calculate from the legal part and illegal part with different identities overhead time, we can apply the k- means cluster analysis to the mixture of these two ToA streams. Due to the assume analysis, the distance between comprise nodes is long enough. We explore the k-means algorithm, which aims to partition n observations into k clusters. The ToA is chosen as the dissimilarity measure. In our scheme, k is equal to 2. It is obvious that the legal and illegal neighbors will aggregate two clusters. This mechanism will detect the wormhole attack in sensor. For long run detection system in sensor network we will do some packet header changes in sensor network. We will introduce packet counter (forward, receive, sent) and next hop address in table which is attached with packet header. Each node will proceed with this mechanism with K-means detection algorithm scheme. Hybrid Scheme will work for detection and long term prevention of wormhole attacks in Sensor network.

V. OBJECTIVES

To fulfill our require experimentation we will have following objectives

- Detection and Avoidance of Wormhole attack in wireless sensor network.
- To develop Long term prevention mechanism for sensor communication.

VI. METHODOLOGY

Our research will start with study of sensor network implementation and will proceed with Detection and avoidance of wormhole attack for sensors in following steps.

1st Phase: This phase will contain the basic functionality and collection of information (simulator, basic sensor functions etc).

2nd Phase: In this phase we will create a wormhole attack in sensor network and will fetch the difference in the performance of the Sensor network.

3rd Phase: We will implement the proposed scheme to avoid the wormhole attack. To avoid the wormhole attack, proposed algorithm will be implemented in scenario affected by wormhole attacks and this will try to normalize the scenario to its original state. In Neighbor discovery each node records the time init T and broadcasts a HELLO message for the neighbor discovery immediately after the deployment of the sensor nodes. Each node that receives a HELLO message sends a reply. Each node builds its neighbor list which could include remote neighbors connected by a wormhole and calculate the time of arrive (ToA) overhead. Packet header will carried the packet forward, packet sent, packet received, time to live and next hop address filed. In case of wormhole detection, drop packet field will increase

more than normal count. If it is more than threshold number decided then it is consider being the malicious node. The basic idea behind using the k-means cluster analysis to detect wormhole attack relies on the distance correlation in the physical locations of nodes. According to the ToA calculate from the legal part and illegal part with different identities overhead time, we can apply the k-means cluster analysis to the mixture of these two ToA streams. Due to the assume analysis, the distance between comprise nodes is long enough. We explore the k-means algorithm, which aims to partition n observations into k clusters. The ToA is chosen as the dissimilarity measure. In our scheme, k is equal to 2.

4th Phase: Final step will be comparing of the proposed schemes with wormhole hitted scenario. Parameters for comparison will be number of hops, throughput, Traffic dropped.

VII. EXPERIMENTAION

Basic parameters used for experimentation. Some of the experimentation done for checking the behavior of AODV protocol under wormhole attacks are given below:

Parameters	Value
Simulator	OPNET
Simulation Time	900
No of nodes	50
Routing Protocol	AODV
Traffic Model	CBR
Pause Time	100 sec
Speed	11 mps

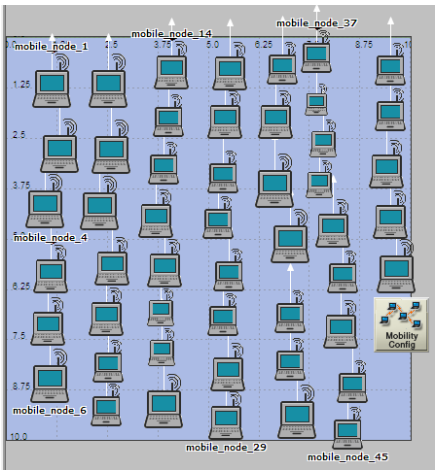

Figure.1. Simulation of AODV with and without wormhole attacks

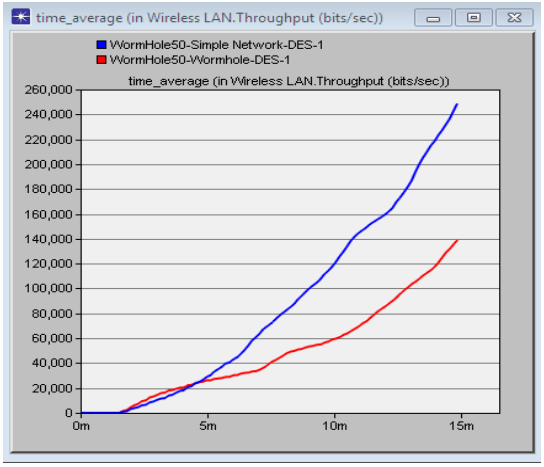

Figure.2. Throughput variation

The variation of the throughput from normal and wormhole attack scenario.

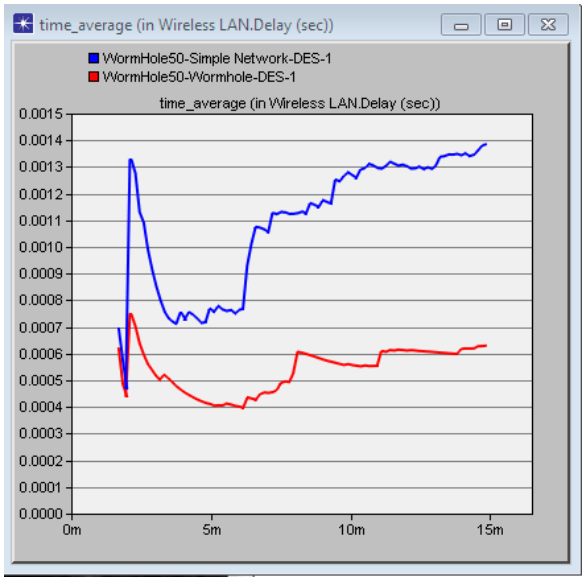

Figure.3. Delay variation of wormhole and normal network

The variation of the delay in case of wormhole and normal scenarios.

In above experimentation we have considered AODV protocol with 40 mobile nodes and application Traffic used is HTTP. Wormhole attack has been implemented and simulation shows the variation in throughput (Figure.2) and delay (Figure.3) in both cases. At initial stage throughput increased in case of Wormhole attacks but decreases gradually. Delay shown in wormhole scenario is low as compared to simple network. This experimentation shows the behavior of protocol under attacks. Further experimentation would be on preventing the attacks and have more attacks experimentation.

VIII. CONCLUSION

This Research is our continuous study and we will find the better results in preventing wormhole attack from mobile ad-hoc networks and will prove to be a good solution for saving resources while finding the wormhole attack in Mobile Ad-hoc Network and also will be effective in finding Wormhole attack perfectly. This Research is still in process and experimentation in running phase to test the developed algorithm on Mobile Ad-hoc Networks. A new concept has been developed which can both detect and isolate the wormhole attacks with limited energy used.

REFERENCES

[1] Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi.,"Elimination of Wormhole with Multipath Algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol.1, Issue.2, pp.34-38, December 2011.

[2] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review" An International Journal on Engineering Science and Technology, Vol.2, No. 2, pp 65-69, April 2012.

[3] Routing protocols and concepts, CCNA exploration companion guide. ''Introduction to dynamic routing protocols''. Chapter three, pp 148-177.

[4] Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology, Vol.2, No. 2, pp 84-89, August 2012.

[5] R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 37-41, November 2011.

[6] Phuong Van Tran, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", IEEE Conference on Consumer Communications and Networking, Vol.4, No.8, pp.93-98, January 2007.

[7] Turgay Korkmaz, "Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, International Journal of Information Technology , Vol. 2, No. 2, pp 704-709, April 2005.

[8] Van Phuong T., Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, Heejo Lee, " Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Conference on Asia-Pacific Service Computing Conference, pp 172- 178, December 2007.

[9] Ma Hongwei, "The Study on Ad hoc Networks Security Strategy based on Routing Protocols", IEEE International Conference on Computer Science and Network Technology, Vol.1, No.4, pp 445-449, December 2011.

[10] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj, B.Prabhu, "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks" IEEE International Conference on Information Theory and Aerospace & Electronics Systems Technology, pp 1–5, March 2011.

[11] Ms. N.S.Raote, Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies, Vol.2, No. 2, pp 172 – 175, June 2010.
[12] Dr. Karim Konate, Abdourahime Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking, Vol. 4, No. 2, pp 156-158, June 2011.
[13] Reshmi Maulik, Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, Vol. 3, No. 1, pp 271-279, January 2011.
[14] Lijun Qiana, Ning Songa, Xiangfang Lib," Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach", Journal of Network and Computer applications, Vol.8, No.4, pp.456-469, 2005.
[15] A.Vani," A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering, Vol.3, No.6, pp.23-29, June 2011.
[16] Vaidya B,"Secure multipath routing scheme for mobile ad hoc network", In Proceedings of IEEE International Symposium on Dependable, Autonomic and Secure Computing, Vol.3, No.3, pp.163–171, 2007.
[17] Ye Z., Krishnamurthy V.,"A framework for reliable routing in mobile ad hoc networks", In Proceedings of the IEEE INFOCOM Conference, Vol.1, pp.270–280, Mar. 2003

