Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.7 – 10

REVIEW ARTICLE

A Review of Wormhole Detection Using HMM Approach

Himani Deswal[1], Rahul Yadav[2]

[1]Computer Science and Engineering Department, PDM College of Engineering, Bahadurgarh, Haryana, India

[2]Assistant Professor of Computer Sciences, PDM College of Engineering, Bahadurgarh, Haryana, India

[1] csehimani.deswal14@gmail.com; [2] rahul_engg@pdm.ac.in

Abstract— Mobile network is one of most common ad hoc network with lot of problems related to congestion and routing. 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. A specific attack called the Wormhole attack 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. In this proposed approach we will present a handshaking mechanism along with Hidden Markov Model (HMM) to detect the wormhole attack in a network. According to this approach the validity of a node will be identified by performing the authentication mechanism and the communication support will be identified by HMM.

Key Terms: - Mobile ad hoc network; wormhole attack; routing protocols; Hidden Markov Model

I. INTRODUCTION

In cryptography, the most focus area of research in mobile ad hoc networks is to provide a trusted environment and secure communication. There are several applications of ad hoc network which need highly secure communication. Some of the example of these applications are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation such as after natural disaster like a flood, tornado, hurricane and earthquakes. There are basically three types of routing protocols: reactive routing protocol, proactive routing protocol and hybrid routing protocol. Here, we emphasis on AODV and DSR routing protocols which are the part of reactive routing. In this paper we define the wormhole attack and a new general and effective mechanism for detection and then defend against wormhole attack. The wormhole attack is a severe type of attacks in which two malicious nodes can forward packets through a private "*tunnel*" in the network as shown in Figure:

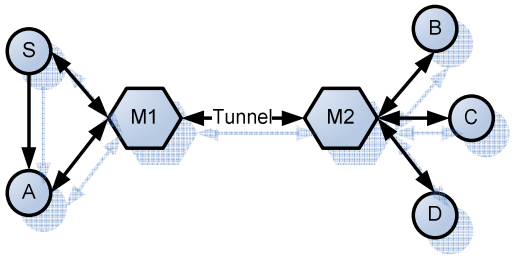

Figure 1: Wormhole attack

Here, M_1 and M_2 are two malicious nodes which link through a private connection. Every packet that M_1 receives from the network is forwarded through "*wormhole*" to node M_2, and vice versa. This attack 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.

In wormhole attack the attacker record the packets (bits) at one location and them in another location in same network or in different networks. The attacker can transfer each bit directly, without waiting the entire packet. It is very difficult to find out the location of wormhole attack without having the cryptographic key or without knowing the infrastructure of routing protocols. Wormhole makes the tunnelled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc.

In this proposed approach we will present a handshaking mechanism along with Hidden Markov Model to detect the wormhole attack in a network.

II. RELATED WORK

In year 2006, Yih-Chun Hu[5], has defined a work on wormhole attack in sensor network. According to his work in the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many adhoc network routing protocols and location-based wireless security systems. For example, most existing adhoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. He presented a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and he presented a specific protocol, called TIK, that implements leashes.

In year 2009, Majid Khabbazian[6], analyzed the effect of the wormhole attack on shortest-path routing protocols for wireless ad hoc networks. Using analytical and simulation results, he showed that a strategic placement of the wormhole when the nodes are uniformly distributed can disrupt/control on average 32% of all communications across the network. He also analyzed a scenario in which several attackers make wormholes between each other and a case where two malicious nodes attack a target node in the network. He showed how to evaluate the maximum effect of the wormhole attack on a given network topology. Then, we compute the maximum effect of the wormhole attack on grid topology networks and show that the attackers can disrupt/control around 40% to 50% of all communications when the wormhole is strategically placed in the network. Finally, to defend against the wormhole attack, he proposed a timing-based countermeasure that avoids the deficiencies of existing timing-based solutions.

In Year 2010, Jinsub Kim performed a work," Timing-based Localization of In-Band Wormhole Tunnels in MANETs"[9]. This paper begins with binary hypothesis testing, which tests whether a suspected path is carrying tunneled traffic. The detection algorithm is presented and evaluated using synthetic voice over IP (VoIP) traffic generated in a network test bed. After that, Author considers multiple hypothesis testing to find the most likely tunnel path among a large number of candidates. Author presents a tunnel path estimation algorithm and its numerical evaluation using Poisson traffic.

Jin Guo, Zhi-yong Lei[2], has proposed A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification. They presented a kind of wormhole attack defense strategy of WSN based on neighbor nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbor nodes to avoid Wormhole attack effectively. Modeling and simulation of WSN based on OMNeT++ shows that the AODV added neighbor nodes verification successfully implement effective defense.

In year 2011, Mariannne. A. Azer [3], has proposed Wormhole Attacks Mitigation in adhoc network. He proposeed a scheme for the wormhole attack prevention. The scheme relies on the idea that usually the wormhole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the wormhole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing.

In year 2011, Pallavi Sharma Prof. Aditya Trivedi [4], have proposed An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature. In this paper, she present a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of

verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

In the year 2011, Saurbh Gupta, Subrat Kar and S Dharamraja[1], has work on wormhole detection using Hound Packet. They present a protocol for detecting wormhole attacks without use of any special hardware such as directional antenna and precise synchronised clock and the protocol is also independent of physical medium of wireless network. After the route discovery, source node initiates wormhole detection process in the established path which counts hop difference between the neighbours of the one hop away nodes in the route. The destination node detects the wormhole if the hop difference between neighbours of the nodes exceeds the acceptable level.

In Year 2012, Daniel Winograd-Cort[12], performed a work," This paper better motivates, expands upon, and formalizes the notion of a wormhole to fully unlock its potential. Author show, for example, that wormhole can be used to define the concept of causality. This in turn allows us to provide behaviors such as looping, a core component of most languages, without building it directly into the language. Author also improves upon Presented previous design by making wormholes less verbose and easier to use. To formalize the notion of a wormhole, Author defines an extension to the simply typed lambda calculus, complete with typing rules and operational semantics.

III. THE PROPOSED ROUTING PROTOCOL

In this proposed approach we are presenting a handshaking mechanism to detect the wormhole attack in a network. According to this approach a node will request to its neighbouring nodes and perform a request and response mechanism. The node will maintain the table to track the timeout. If the reply time is not accurate there is some attack in the network. To resolve the problem of wormhole attack we can perform a cryptographic handshaking. It means only the authenticated node will get the request and can reply properly i.e. the cryptographic handshaking will avoid the fake reply from a node and node reliability will be achieved.

Once the authentication is proven, the next work is the implementation of the Hidden Markov Model to perform a predictive and probabilistic analysis of throughput and the response time between all pairs over the network. The all pair communication analysis will be done up to two level of communication that can effectively analyze the tunnel attack over the network. Once the attack will be detected, the next work is to block these nodes and to perform a reliable communication over the network for a safe path so that no attacked node will be the part of communication path.

The analysis will be done in terms of packet transmission received and the packet lost over the network. The route safely and reliability are the major objective of this defined work.

IV. CONCLUSION

Wormhole attack 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 wormhole 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.

ACKNOWLEDGEMENT

Assistant Prof. Rahul Yadav is the assistant professor in Department of Computer Science and Engineering at PDM College of Engineering, Bahadurgarh, Haryana. I am specially grateful for his guidance and contributions by generously giving his time and carefully reviewing this manuscript.

REFERENCES

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

[2] 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

[3] Mariannne. A. Azer, “Wormhole Attacks Mitigation”, 2011 Sixth International Conference on Availability, Reliability and Security

[4] 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

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

[6] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 2, FEBRUARY 2009

[7] Gurjinder Kaur, Yogesh Chaba, V. K. Jain, in their research paper" Distributed Denial of Service Attacks in Mobile Adhoc Networks" 2011.

[8] Shideh Saraeian, Fazllolah Adibniya, Mohammad GhasemZadeh and.SeyedAzim Abtahi ,in their research paper "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET" 2010

[9] M. Ostaszewski, F. Seredynski, and P. Bouvry, "Coevolutionary-based mechanisms for network anomaly detection," Journal of Mathematical Modelling and Algorithms, 6(3) 2007 pp. 411–431.

