Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 6 Issue 1, January - 2019

A Survey on Detection and Prevention of Wormhole Attack in Mobile Ad Hoc Networks

Anju-man-ara
Dept. of Information & Communication Engineering
Rajshahi University
Rajshahi, Bangladesh
anjuman77@gmail.com

A.S.M. Shahabuddin
Dept. of Physics,
Rajshahi University
Rajshahi, Bangladesh
asms_sagor@yahoo.com

***Abstract*—The mobile ad hoc network (MANET) consist of a collection of self-organized mobile nodes. In these networks, each node acts as a host as well as a router. The security of MANET is prone to various attacks due to lack of central administration and multi hop routing communication process. Wormhole attack is one of them. Wormhole attack makes a tunnel between attacker nodes and passes the packets through the tunnel. This article reviews mainly various approaches to detect and prevent wormhole attack in these networks.**

Keywords—Mobile ad hoc network, wormhole attack, proactive routing, reactive routing.

I.Introduction

Literally, the word “Ad hoc” means “for this purpose only”. These wireless networks are self-configured and do not follow any fixed infrastructure. Quick communication is provided by mobile ad hoc networks (MANETs) to transfer the packets from one node to other. A MANET is an autonomous ad hoc wireless network consisting of independent nodes. It is different from cellular wireless networks in the way that it does not require static or fixed infrastructure and no centralized control can be available. In this network, one node can communicate with other nodes either directly when they are in radio range of each other or via intermediate mobile nodes because of flexibility that a MANET offers and the network can be built at anywhere, at any time, as long as two or more nodes are connected and communicate with one another. Since MANETs have flexibility [16], auto configuration capability and lack of infrastructure, ease of maintenance, self-administration capabilities and cost effectiveness, MANETs have become an integral part of next generation network.

Due to its openness and lack of conventional techniques of management MANET is prone to various attacks like wormhole, rushing, jellyfish attack etc. Routing protocols are needed in MANET to route packets from source to destination, Ad hoc network routing protocols are categorized into 3 types proactive, reactive and hybrid [1,3]. Proactive routing protocols are those where all the nodes store routing information about other rode in the network and routing information updated periodically. Example of this type of routing protocol is destination sequenced Distance vector (DSDV) routing protocol.

In reactive routing protocol, route between nodes are searched when communication is initiated. Route discovery process is used to search route through flooding RREQ message. RREQ message is propagated until it reaches the destination. Then destination replies by sending RREP message to the source in the reverse path. In this way path is established. Example of reactive routing is ad hoc on demand Distance vector (AODV) routing protocol. The hybrid routing protocols are combination of both. Different types of wormhole attacks and techniques of detecting and preventing wormhole attacks in MANET are discussed in this paper.

The remaining portion of the article has been arranged as follows: section-II discusses about wormhole attack and its classification. Section-III provides different performance metric that are affected by wormhole attack. In Section-IV, different methods to detect and prevent wormhole attack are described.

II.Wormhole Attack and its Classification

Wormhole attack is one in which attacker nodes create a tunnel in between them to analyze the traffic through the network or to drop packets selectively or completely to affect the flow of information. There may be two or more attacker nodes in wormhole attack. The Two malicious nodes form the tunnel and capture the traffic as shown in Figure-1. In figure-1 node B and C are attacker nodes. Suppose node S wants to send data to D, then node B (malicious) tunnels that packet to another malicious node C and C may send packet to D or may drop it.

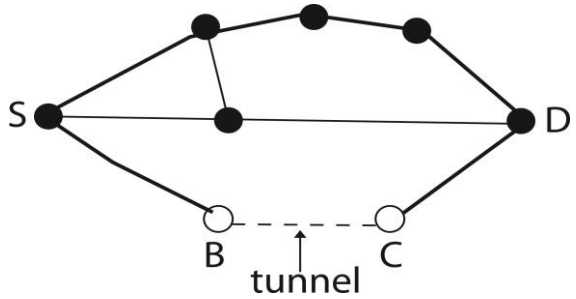

Figure-1 Wormhole attack

There are three types of wormhole attacks-the open attack, the half open and the closed attack as discussed in [5].

Open wormhole attack:

Here all nodes involved at the end of the wormhole tunnel are known to the other nodes in the network.

Half open wormhole attack:

Here one malicious node is known but the other is unknown to the legitimate nodes in the network.

Closed wormhole attack:

This attack is also called hidden attack. The legitimate nodes do not know about the existence of malicious nodes because this attack does not update the packet header at the time of route discovery process.

Wormhole attacks can be classified in another way:

(1) Threshold based wormhole attack:

This type of attack will drop all the packets whose size are greater than or equal to the threshold value.

(2) All pass based wormhole attack:

This type of wormhole attack passes all the packets irrespective of their size.

(3) All drop based wormhole attack:

In this type of attack, all packets are dropped irrespective of their size.

III.Performance metric

The performance of MANETS is determined by several parameters (metric) such as throughput, packet delivery ratio, end-to-end delay and normalized routing load.

i. Throughput

Throughput is defined as the ratio of total number of packets delivered to the total simulation time. It is measured in packets per second.

Mathematically,

$$\text{Throughput} = \frac{Total\ number\ of\ packets\ delivered}{Total\ simulation\ time}$$

ii. Packet Delivery Ratio (PDR)

The packet delivery ratio is defined as the ratio of the number of packets received by the destination to the number of packets originated by the source.

Mathematically,

$$\text{PDR} = \frac{Number\ of\ packets\ received\ by\ the\ destination}{Number\ of\ packets\ originated\ by\ the\ source}$$

iii. End-to-End delay (E-To-E)

The average time acquired by the packets to pass through the network is called end-to-end delay.

iv. Normalized Routing Load (NRL)

It is the number of routing packets broadcasted per data packet which is successfully received by the destination node.

IV.Methods to defend wormhole attack

Various detection and prevention techniques of wormhole attack have been proposed till now.

In [17], the major metric is the number of links that connect source and destination (i.e. path length). The problem here is that it is able to detect encapsulation type wormholes only and it cannot detect when the wormhole path length is equal to or less than 4 hops.

The article in [6] detects wormhole attack in MANET based on absolute deviation covariance. This method increases computational complexity and it also requires additional information to be known in prior.

In [18], a coordinator is used to detect and mitigate attack. Here overhead is increased due to examination of multiple messages between coordinator and other nodes.

The authors in [7] proposed various approaches such as packet leash, round trip time based approach, cluster based hierarchical addressing approach, distributed algorithm using graph information and trust based approach.

In [8], the proposed algorithm combines a black hole detection behavior mechanism and a wormhole detection behavior mechanism to detect and prevent vulnerabilities in MANET based on the way of behavior. This article combines transmission radiation based and 3 phased approach using time factor.

In [9], they use a new detection mechanism called RTT-TC, which is based on round trip time measurements and topological comparison (TC). They evaluated their scheme with MANET running ad hoc on demand distance vector (AODV) routing protocol. In this article neighbor list is created based on the idea that a wormhole tunnel induces packet latency. Whenever the RTT between two nodes is more than k times of their respective RTTavg, they suspect a wormhole tunnel exist between them.

In [10] a wormhole detection and prevention technique has been proposed which is based on neighbor node and hop count method. Proposed algorithms check the validity of route suggested by AODV protocol whether the route is infected by wormhole attack or not on the basis of some threshold.

In [11], the proposed system effectively modifies AODV with the ability to detect and prevent the sinkhole and wormhole attack, so the modified protocol is named Attack Aware Alert (A3AODV). The experiment is carried out using NS2 simulator and the result shows the efficiency in terms of packet delivery ratio and routing overhead.

The article in [12] mainly focused on different security attacks in AODV routing algorithms in MANETs along with their comparison on various parameters. They studied and simulate the AODV routing protocols under the wormhole and DOS attacks to a certain level and they found that because it has drawbacks such as less throughput, low packet delivery ratio and high network routing overhead. Small network is more vulnerable for these attacks.

In [13], they proposed a trust and reputation management scheme to find out the trusted location in MANET environment. Evaluating RREQ trustworthiness in MANET still remains as an open problem still now. To evaluate trusted location, they introduce trusted and reputation based mechanism applying base station.

The authors in[14] proposed a technique which discovers an alternative route to the target node. Because the shortest path can have the malicious attacker. The implementation of the secure route discovery protocol is performed using NS2 and by the notification of the AODV routing protocol.

In [15], the proposed security approach is to detect and mitigate wormhole attack. It is secured AODV approach which efficiently finds wormhole attack present in MANET and digital signature is used to prevent it. This approach is based on a calculation of tunneling time taken by tunnel to analyze the behavior of wormhole attack. A digital signature and hash chain algorithm is used to mitigate the wormhole node.

V.Conclusion

Security of MANETs is a challenging issue as the nodes are mobile and self-organized. Although many researchers have worked for security of MANET, but the area of research is still open. Many techniques have been designed to detect and prevent wormhole attack in MANET. In this paper, we have discussed some of the possible techniques

References:

[1] C.Siva Ram Marthy and B S Manoj, "Mobile Ad Hoc Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5, 2004.

[2] Theodore S. Rappaport, "Wireless Communication" Prentice Publisher, ISBN 0133755363, January 1994.

[3] Yongguang Zhang and Wenke Lee, Security in MANETs, in Book Ad Hoc Networks Technologies and protocols, Springer, 2005.

[4] Jangral, A.Goel, N. Priyanka and Bhati, K.- Security Aspects in Mobile Ad Hoc Networks(MANETs): A Big Picture, International Journal of Electronic Engineering, pp. 189-196, 2010.

[5] Priya Maidamwar and Nekita Chavchan, " A survey on security issues to detect wormhole attack in wireless sensor network", International Journal on Ad Hoc Networking Systems(IJANS) Vol. 2, No. 4, October 2012.

[6] Sayan Majumdar, Prof. Dr. Debika Bhattacharyya, "Mitigating Wormhole Attack in MANET using Absolute Deviation Statistical Approach", IEEE 8th Annual Computing and Communication Workshop and Conference,pp 317-320,2018.

[7] Roshani Verma, Prof. Roopesh Sharma, Upendra Sing," New Approach through Detection and Prevention of Wormhole Attack in MANET, Internation Conference on Electronics,Communication and Aerosace Technology, ICECA 2017,pp 526-531, 2017

[8] Thanuja.R,Sri Ram.E, Dr.A.Umamakeswari,"A Linear Time Approach to detect wormhole tunnels in MANET using 3PAT and Transmission Radious(3PATw)",Procedings of the second International Conference on Inventive System & Control(ICISC 2018), PP-837-843,2018.

[9] Mohammad Rafiqul Alam, King Sun Chan,"RTT-TC: A Toological Comparision Based Metod to Detect Wormhole Attacks MANET",IEEE Communication Surveys and Tutorials, 2010.

[10] Gaurav Sharma, Mehjabeen Fatima,"An Enery Efficient Approach for Wormhole Detection,International Journal of Computer Applications(0975-8887),Vol 76-No.17, 2013.

[11] D.Sasirekha, Dr.N.Radha,"Secure and Attack Aware Routing in Mobile Ad Hoc Networks Against Wormhole and Sinkhole Attacks",Proceedings of the 2nd International Conference on Communication and Electronics Systems(ICCES 2017),ISBN:978-1-5090-5013-0,pp-505-510,2017.

[12] Brijendra Kumar Joshi and Megh Soni,"Security Assessment of AODV Protocol under Wormhole and DOS Attacks",2016 2nd International Conference on Contemporary Computing and Informatics(ic3i),pp-173-177, 2016.

[13] Shabina Parbin, Leeladhar Mahor,"Analysis and Prevention of Wormhole Attack Using Trust and Reputation Management Scheme in MANET", 2nd International Conference on Applied and Theoretical Computing and Communication Technology, pp-225-228,2016.

[14] Chitra Gupta, Priya Pathak,"Movement Based or Neighbor Based Technique for Preventing Wormhole attack in MANET", 2016 Symposium on Colossal Data Analysis and Networking (CDAN)", 2016.

[15] H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wandra,"Advanced AODV Approach For Efficient Detection and Mitigation of Wormhole Attack in MANET", 2016 Tenth International Conference on Sensing Technology,2016.

[16] Roy, Radhika Ranjan,"Handbook of Mobile Ad Hoc Networks for Mobility Models",http://www.springer.com/gp/book/9781441960481.

[17] Mohammad Rmayti, Lyes Khoukhi, "Graph-based wormhole attack detection in mobile ad hoc network",conference paper : February 2018, Research gate.

[18] R.Arun, Prakash, W.R. Salem,Jeyaseelan and T.Jayasankar,"Detection, Prevention and Mitigation of Wormhole attack in Wireless ad hoc network by coordinator",Applied Mathematics and Information Sciences-An International Journal-Appl.Math Inf.Sci 12, No 1, 233-237(2018).