International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 9 September 2018

Approach through Detection and Prevention of Wormhole Attack in MANET

Aditi Dawane[1], Harsha Verma[2], Mayank Bhatt[3]
PG Scholar, Dept of CSE, Lakshmi Narain College of Technology and Science, Indore, MP, India[1]
Asst. Professor, Dept of CSE, Lakshmi Narain College of Technology and Science, Indore, MP, India[2]
HOD, Dept of CSE, Lakshmi Narain College of Technology and Science, Indore, MP, India[3]
dawane.aditi@gmail.com[1], harshavermaa@gmail.com[2], mayankbhatt27@gmail.com[3]

Abstract: *A mobile ad hoc network (MANET) is a dynamic wireless network that can be fashioned without any pre-existing infrastructure in which every node can act as a router. MANET has no clear line of defense, so, it is available to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the most important challenges in MANET is to sketch the sturdy security answer that can guard MANET from worm-hole attack. Different mechanisms have been proposed the usage of digital signature methods to countermeasure the routing attacks against MANET. However, these mechanisms are no longer suitable for MANET aid constraints, i.e., limited bandwidth and battery power, due to the fact they introduce heavy traffic load to exchange and verifying keys. In this paper, the cutting-edge protection issues in MANET are investigated. Particularly, we have examined wormhole attack as well as existing options to defend MANET protocols.*

Keywords: *MANET, WORMHOLE attack, Malicious node and Prevention.*

1. INTRODUCTION

Structure of MANET is comprises of portable and independent nodes which does not have focal framework to deal with their part. These kinds of systems are exceptionally agent to have correspondence by nodes which are out of region of remote transmission scope. MANETs are use in numerous fields, which require having extensive variety of scope, use zones illustration, for example, ecological control [1], strategic territory, for example, military combat zones [2], instruction zone, for example, college grounds [3], home and endeavor systems administration, for example, meeting rooms and gatherings. Figure 1 appears, the hubs are moving by utilizing air as a medium to exchange and speak with alternate gadgets, and this is the reason for genuine security issues contrasted with wired system.

Figure 1: Typical MANET

Anyway it has a few shortcomings, for example, nodes need to remain in scope of correspondence because of restricted radio flag extend. Signs can square or ingested subsequent to hitting to a few items. Portable nodes have restricted existence of battery, if the node correspondence and transmission is preceded for long time it diminished the life of battery and node can't play out the obligations and sooner or later going latent in the system. This work is done to know data about wormhole attacks and the systems to identify and keep the wormholes in the system. We survey numerous past related works and needs to discover who we

can have a decent protection component to recognize wormholes. We have to accomplish better security in the system against the wormhole attacks to enhance wormhole identification rate, and in addition accomplish more prominent throughput and less normal postponement.

MANET has several challenges. They include:-

Power awarenes*:* Since the nodes in an Ad-hoc network usually run on batteries and are deployed in opposed terrains, they have stringent energy requirements. Show up smaller, one giant attribute of cluster-based routing is that it can make a dynamic topology appear less dynamic. In order to put in force a dynamic hybrid routing scheme, efficient clustering algorithms must be designed.

Dynamic topology: The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time.

Quality of service (QoS) – Providing constant QoS for different multimedia services in frequently changing environment.

Multicast Routing – Designing of multicast routing protocol for a constantly changing MANET environment.

Security*:* Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity, authenticity and non-repudiation are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

Distributed network*:* A MANET is a distributed wireless network without any fixed infrastructure.

2. WORMHOLE ATTACK

In Wormhole Attack, two or more malicious attacker receives data packets from one place of network, forwards them through the wormhole tunnel and releases them into another location which offers two far away nodes the illusion that they are shut to every other. For higher perception let us think about a multi-hop Ad hoc community irrespective of whether nodes in community are mobile or static as shown in (Figure 2). In this figure, a node or a person of network is denoted by circle whereas line represents the connection between the two nodes. Suppose node 2 wishes to transmit message to node 9. But before sending message, supply node will determine a course to ship message by means of the usage of Predefined Routing Protocols which may also be Proactive or Reactive in nature. If node 2 that is source node had already maintained a routing table (i.e. proactive routing) then it will maintain routing information regarding each and every node in network which will be used to send message to destination but if source node uses reactive routing protocol then it will no longer have any routing table hence it needs to discover routing statistics earlier than transmitting any message. In Reactive routing protocol sender publicizes a RREQ message to its one-hop away neighbors in network. All nodes that get hold of RREQ message will take a look at whether RREQ is supposed for itself or not and if no longer then it will retransmit RREQ message after altering its node identity in message and when request message is obtained through destination node it will unicast route reply message with route data to sender thru same route from which request message had arrived to node. Mostly routing protocols decide route that is shortest because of nodes in ad hoc community have confined bandwidth and power. Hence we can say the node 2 will ship the message via the node 2-5-6-8-9.In the network, the intermediate nodes act as routers that send the message to destination. Let us count on that ad hoc network referred to above is below wormhole attack. Suppose that two attackers are placed in neighborhood of node 2 and node 9 and these attackers are connected with each other through a excessive speed bus. It may additionally be viable that attacker may additionally no longer be part of community but still it can overhear message due to the open nature of ad hoc network. Whenever any of attackers receives message transmitted with the aid of nodes on whose vicinities attacker lies, retransmission of message is done by using the other attacker in network. Thus nodes where an attacker lies which are node 2 and node 9 are made to consider that each of them are linked to every different directly. Hence a fake link is created with the aid of the attacker in a community i.e. between node 2 and node 9. Due to this fake hyperlink node 2 will ship message to node 9 immediately thru wormhole tunnel. Hence now the route is 2- 9. All routes in community that had to pass thru node 2-5-6- 8-9 are now changed with the aid of node 2-9. Hence maximum numbers of messages in community are directed through wormhole which puts the attacker in a very powerful function as compared to different nodes in the network. Attacker can misuse the faux link by means of storing all messages passing thru it which can be used to analyze content material even if the attacker has no cryptographic keys. Attacker can additionally selectively drop or alter the message of any node at any time which influences the availability and integrity elements of security. Thus Wormhole attack is dodging for more assaults like eavesdropping, congestion, spoofing packet loss and so on

[5]. Wormhole assault is one of the Denial-of-Service assaults which have an effect on the network even except the knowledge of any cryptographic techniques. That is why wormhole assault is very difficult to detect. It can be launched by means of two or greater nodes. In two ended wormhole, packets are tunneled through wormhole link from supply to vacation spot node and on receiving packets, destination node retransmit them to the different end.

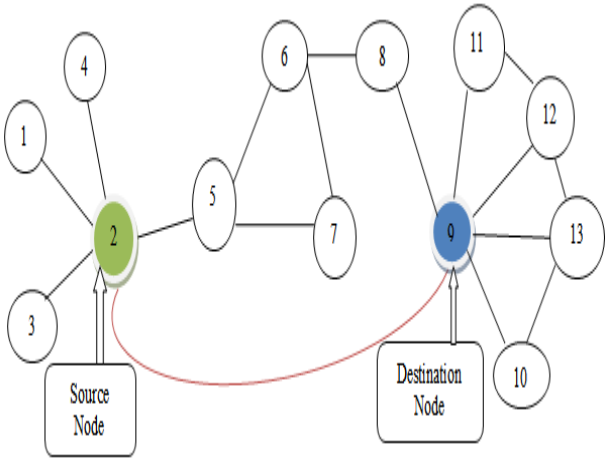

Figure 2: Wormhole Attack in Ad-hoc Network

3. RELATED WORK

Various Detection and Prevention Techniques have been proposed in order to obtain security against the wormhole attacks.

Packet Leashes

Yhi-Chun et. al. [7] proposed a mechanism for detecting the wormhole attacks, primarily based on the temporal and geographical leashes. In Temporal leashes, all nodes require a synchronized clock and these are used as sending and receiving methods. While in case of geographical leashes, there is no need of any synchronized clock. It makes use of the GPS hardware.

Directional Antennas

L.Hu et. al. [8] used the mechanism in which the directional antennas are used for verbal exchange between the nodes. It is the hardware based totally approach. But, this technique fails if an attacker deliberately places the wormhole hyperlink between the communicating nodes.

Digital Signatures

Pallavi Sharma et.al. [9] proposed a technique a to notice and stop the wormhole attack by using the usage of the approach of digital signatures. According to this method, each and every node has digital signatures of each and every different node. In this way, a verification mechanism is carried out when the receiving node can verify the sending node through its digital signatures. So, a trusted course is created between the source and the destination and the attacking node can be without problems identified.

Neighbor Node Analysis

Sweety Goyal et. al. [10] introduced a way of examining the neighbor nodes for the reason of authentication. Every node will analyze all the different neighbor nodes. In this method, a node will send a request message (RREQ) to the neighbor nodes. All the nodes after receiving the request message will send the reply message (RREP) to the sending node. This method is based on the contrast between the response time of RREP sent and the true RREP time. If response time of genuine RREP is greater than the RREP despatched plus the threshold value, it can be said that the wormhole link is current in the network.

DelPHI Technique Delay Per Hop Indication

Lui K.S et.al.[11] calculates the delay per hop of the disjoint paths. The lengthen per hop is calculated for each and every path. It has been validated that prolong per hop value for a professional course is always shorter than the wormhole path. So, if the fee of lengthen per hop is extremely high, then it can be concluded that it is the wormhole path existing in the network.

4. CONCLUSION

As there is increasing threats of attacks on the mobile network, MANETs need to have a impenetrable way of transmission and conversation and this pretty difficult and quintessential issue In this paper we study the wormhole attack on routing protocol in MANETs. In this section the worm-hole attack is greater nice in MANETs. This is due to the truth that in worm-hole attack the attacker forcefully makes himself an intermediate node on a chosen route. Due to this the attacker is almost constantly in a position to launch an attack all through the conversation process.

REFERENCES

[1] Nakamura, M., A. Sakurai, and J. Nakamura, Autonomic Wireless Sensor/Actuator Networks for Tracking Environment

Control Behaviors. International Journal of Computer Information Systems and Industrial Management Applications, 2009. 1: p. 125-132.

[2] Amanowicz, M., et al. A trust-based information assurance mechanism for military mobile ad-hoc networks. In Microwaves, Radar, and Wireless Communication (MIKON), 2014 20th International Conference on. 2014. IEEE.

[3] Pal, S., et al. M-learning in university campus scenario-Design and implementation issues. in Industrial Technology (ICIT), 2013 IEEE International Conference on. 2013. IEEE.

[4] Dr.G.Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," In Proceeding of the International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[5] Shaishav Shah and Aanchal Jain, "Techniques For Detection & Avoidance Of Wormhole Attack In Wireless Ad Hoc Networks", In Proceeding of the International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012.

[6] Ali M, et al, "Mitigation of Wormhole Attack in Wireless Sensor Networks", In Proceeding of the Atlantis Press 2012.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

[8] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks". In the Proceedings of network & distributed system Security Symposium,, February 2004.

[9] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", IEEE, 2011.

[10] Sweety goyai, harish rohil, "Securing MANET against Wormhole Attacl using Neighbour Node Analysis" IJCA volume 81,November 2013.

[11] Lui K.-S., Chiu H.S., "DelPHI: Wormhole Detection mechanism for Adhoc Wireless Networks" Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.