ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 2, pp: (19-24), Month: April - June 2020, Available at: www.researchpublish.com

SIGNIFICANT PERFORMANCE AGAINST WORMHOLE ATTACK USING MULTIPATH AODV IN WIRELESS AD HOC NETWORK

Jagrati Dixit[1], Vinita Verma[2], SarveshKumari[3], Abhilash Mishra[4], Ashish Gupta[5]

Research Scholar, Professors, Computer Science & Engineering Dept, NITM, Gwalior India[1,2&3]

Professors, Computer Science & Engineering Dept, NITM, Gwalior India[4&5]

jagratidxt@gmail.com, vini14.verma@gmail.com

Abstract: **In this work the problem of wormhole attack is identified, and solved it using a multi-path-based approach. This multi-path based AODV approach has been implemented to identify and prevent wormhole attack. We have successfully used this scheme to avoid attacks for MANET environments. And we have presented the analysis of performance with proposed and existing and found that proposed model better than existing approach in terms of PDF and THROUGHPUT, and this is also better.**

Keywords: **Worm Hole Attack, AODV, Multipath AODV, MANET, Performance Matrices.**

I. INTRODUCTION

In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. The mobile ad hoc network is vulnerable to various kinds of attacks, among most of the attacks are deployed on the basis of poor routing protocol design. One such critical problem is wormhole attack.

During the wormhole attack, a malicious node captures packets from one location in the network, and with the use of tunnels them to another malicious node at a distinct point, which replays them locally. we have identified two types of wormhole attacks. In the first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the Existence of malicious nodes, just do not know they are malicious. Therefore, there is a need to implement security parameters in order to protect MANETs from malicious users. Due to this type of attack creates the path break problem. so, we considered create this type of problem due to wormhole attack. and solved using Multi-Path based AODV approach.

In this work, we have presented a simulation-based study of the effects of wormhole attacks in MANETs. In this work we have implement Multi path Based AODV Technique For prevention and detection of wormhole attack. And have compared modified metrics using network simulators version 2 and performance metrics such as PDF and throughput with the existing AODV method.

The rest of the paper is organized as follows. In Section 2, we introduce overview of overview of AODV, Section 3 Worm hole attack and Next Sections presents a Problem Statement and solution model multipath methodology to prevent a worm hole attack, result and lastly discussed conclusion.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 2, pp: (19-24), Month: April - June 2020, Available at: www.researchpublish.com

II. OVERVIEW OF AODV ROUTING PROTOCOL

AODV is a reactive routing protocol, discovering routes only when they are needed. In AODV which source node initiates data packet to destination node only when requires the route discovery is occur. There are no periodical exchanges of routing information [16].The Protocol consist of two phases:

Route Discovery: Route discovery is performed through broadcasting RREQ message. Whenever a node needs to send data packets to a destination, it first checks if it has an existing route in the routing table. If not, the source node will initiate a RREQ and broadcast this request to all the neighbors. Then neighboring nodes will update their routing table according to the received message. When RREQ reaches the destination, a RREP will be generated by the destination node as a response to RREQ. The RREP will be transmitted back to the originator of RREQ in order to inform the route. If an intermediate node has an active route towards destination, it can reply the RREQ with a RREP, which is called Gratuitous Route Reply. The intermediate node will also send an RREP to destination node. The RREP will be sent in reverse route of RREQ if a bidirectional link exists.

Route Maintenance: It is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbours about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. Each forwarding node should keep track of its continued connectivity to its active next hops. If a link to the next hop cannot be detected during a period of timeout, a RRER message will be broadcasted to inform the loss of connectivity. On receiving this RRER, usually a local repair will be performed just for maintenance. The expired route will be deleted after the confirmation of its unavailability.

III. WORM HOLE ATTACK

The wormhole attack affects the network routing system; Malicious nodes in these networks create incorrect scenarios on neighbor discovery relationships between mobile nodes. Between malicious nodes, attackers endanger the security of ad hoc routing protocols, creating a direct link. The wormhole tunnel is formed by any two malicious nodes (usually at a distant location) that create an illusion that they are just one hop away and thus route the packets as neighboring nodes. As the wormhole units succeed in making the tunnel, after creating a wormhole tunnel, an attacker receives and copies packets from their neighbors, and then takes them to another raiding attacker through the wormhole tunnel. They can drop packets, replays, tamper packets, or selectively forward them. A malicious node receives a packet at one location in the network, and they receive another at a location in a wormhole attack. The tunnel is between two malicious nodes known as wormholes.

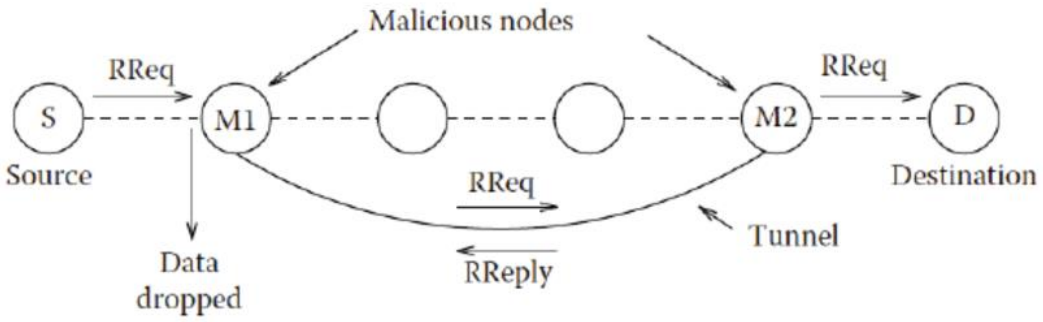

Figure 1: Wormhole attack Problem

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets. Wormhole attack commonly involves two remote malicious nodes shown as M1and M2 in Figure. M1and M2 both are connected via a wormhole link and they target to attack the source node S.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 2, pp: (19-24), Month: April - June 2020, Available at: www.researchpublish.com

IV. PROBLEM STATEMENT

The security of communication in the MANET is important for the safe transmission of information. The absence of any central coordination mechanism and shared wireless medium makes MANET more vulnerable to attacks; there are many attacks that affect MANET. Therefore, we have covered a significant problem wormhole attack in our work. In a wormhole attack, two malicious nodes located far away from each other create a high-speed low latency tunnel between them. A malicious node captures traffic from one area of the network and tunnels it to another malicious node. The traffic received is answered in another area of the network. After this attack an attacker can modify the packet address instead of initiating a continuous data drop with the use of a link break issue.

SOLUTION MODEL: Securing is a very challenging issue for wireless adhoc networks. Understanding the possible form of attacks is always the first step towards developing good security solutions. Wormhole detection has been an active area of research for the past few years. The major function is to detect the presence of a wormhole in the network. Some current protocols detect wormhole attacks but require special planning. This work is intended to develop an identification and prevention model against wormhole attack. The project is to create, detect and prevent a wormhole attack.

Multipath AODV or Modified AODV: The ad hoc on-demand distance vector routing protocol, released by the IETF MANET working group as RFC, is one of the most popular routing protocols. Like other routing protocols, AODV supports single paths. This algorithm uses multiple root discovery procedures in AODV, by which multiple paths are discovered. And by this algorithm searches for multiple paths during the route discovery process, it only picks the best route and leaves the rest. In addition, successive route breakdowns cause intermediate nodes to lose packets because no alternate routes to the destination are available. Therefore, this algorithm is for alternative routes and efficient data delivery and solving the link break problem. This increases overall throughput and packet delivery ratio.

- This problem of wormhole attack is solved using this modification in the AODV routing scheme.
- In the route table file, create a new type of object called multiple route entry. The multiple route entry is an array to keep route entries. The objective of multiple route entry is to keep the routes to the same destination.
- Every method in the AODV main file should change “finding route to the destination” to “finding multiple routes” to the destination.
- The receive request method should be modified to receive the RREQ with the same ID as previous one in order to create the multiple reverse routes.
- The receive reply method should be modified to accept the multiple route reply to create the multiple forward routes.
- The receive reply method should be modified to forward RREP packet to every reverse route.
- The receive error method should be modified to check if the node still has another active route to the destination. If the node still has another active route to the destination, the node no needs to forward the RERR packet.
- Route resolve method for source node should be set to switch from one active path to another active path and switch back in next transmission. The multiple paths will be used to transmit the data packet.

V. SIMULATION PARAMETERS

Simulation Parameters is as follows:

PARAMETERS	VALUE
Routing protocol	AODV
Channel type	Wireless Channel
MAC Type	Mac/802_11
Number of Mobile Nodes	10 to 100
Area	500*500 m^2
Traffic Agent Type	CBR

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 2, pp: (19-24), Month: April - June 2020, Available at: www.researchpublish.com

Node Placement	Random
Simulation time	500s
Connection rate	2 Mbps
Pause Time	1.0s
Seed	1.0
Maximum Speed	10 m/s
Packet Size	512 Byte
Examined approaches	Normal, Attack and Defense

VI. PERFORMANCE METRICS

In this section, we discuss of performance metrics for the protocols:

Packet Delivery Fraction:This is the fraction of number of packets received at the destination to the number of packets sent from the source multiply by 100. In other words, fraction of successfully received packets, which survive while finding their destination, is called as packet delivery fraction.

Throughput: It is the average number of messages successfully delivered per unit time.

VII. SIMULATION MODEL

The NS2 (version 2.31) network simulator has been used for simulation work. The mobility scenarios are generated by a Random waypoint model. The numbers of nodes tested in an area of 500m x 500m for 10 to 100. The simulation parameters are summarized in Above Table. A new routing agent called wormhole AODV is added to include the wormhole attack.

VIII. SIMULATION RESULT AND DISCUSSION

Following the implementation of the proposed security concept for mobile ad hoc networks, this section provides studies about the computation performance of both scenarios. Therefore the performance of the implemented techniques is represented by various parameters. These simulations have used malicious nodes in a network to compare with the normal functioning of AODV. And also presents the performance of the proposed solution which is taken into consideration on the basis of two types of scenarios with and without attacks. In both cases there is an analysis of the effect of network performance with the variation of nodes discussed below using the graphical method. To test the protocol, the NS2 simulator is used. The proposed distributed detection technique is compared with the common wormhole attack scenario without applying any detection techniques in terms of different performance metrics such as packet delivery ratios and throughput.

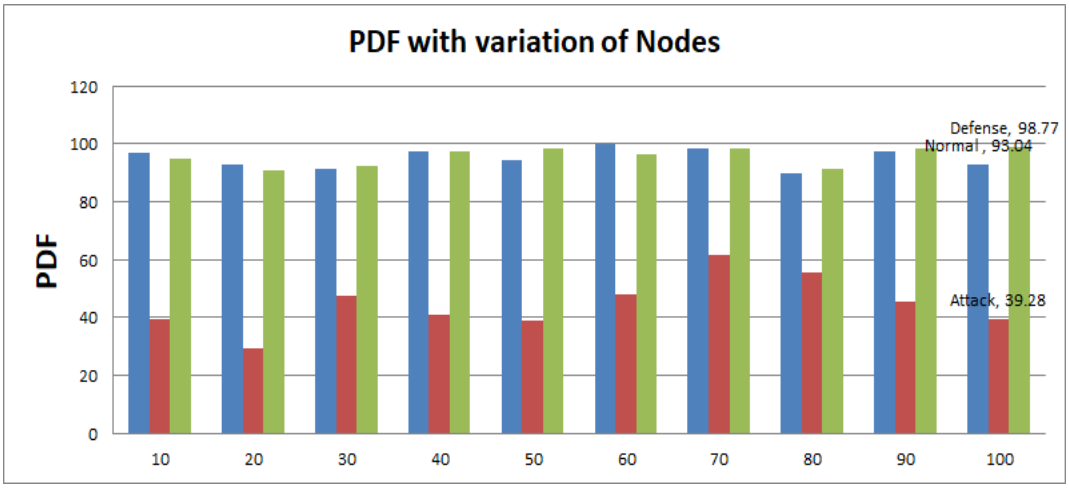

Figure 2: Packet delivery friction with variation of nodes.

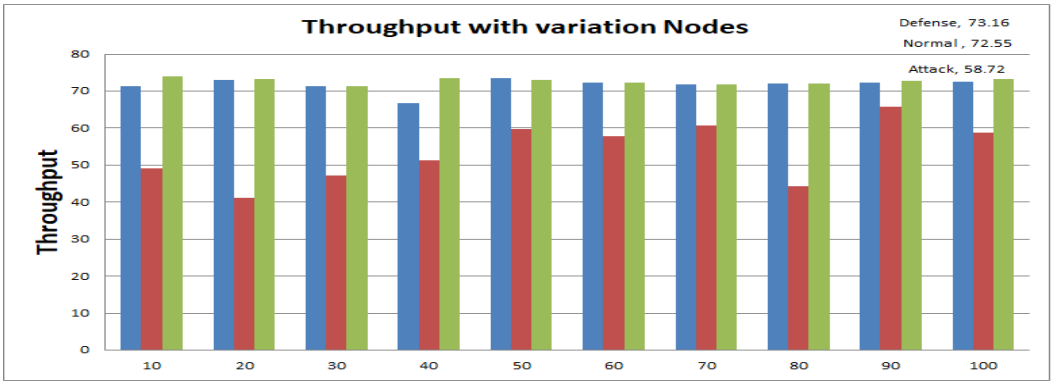

Figure 3: Average Throughput with variation of nodes.

In above Figures, it can be seen that when the network is connected with a wormhole attack, as mobility increases, the number of broken links will also increase, which may lead to more delays in trying to establish a connection. Such a result is also responded to in comments for the number of bytes and packets sent to the destination. And due to more broken connections, the number of bytes and packets received will also be reduced to the normal state, but the modified approach observed is an increase of the performance matrix in terms of the observed PDF and average throughput. We have seen that multipath routing schemes have better results than existing schemes. The average value of the above parameters is shown by the graphical method of the results of the overall simulation.

IX. CONCLUSION & FUTURE WORK

The main advantage of our proposed method is that it avoids a wormhole attack using multipath technique and the receiver can detect that a packet has arrived via some compromised path during the route discovery phase of the AODV protocol. Therefore, it does not require a second phase or periodic checking for the existence of the path during data transmission. The simulation successfully displays for the network scenario. Analysis of simulation results showed that the technique for detecting wormhole attacks in terms of different performance metrics such as packet dropped, packet received and packet delivery ratio is more effective than the normal attacks scenario. Investigations suggest that the proposed detection technique can provide better throughput and packet delivery ratios.

Future work: Future work includes developing more efficient and secure protocols for which the proposed model can be further expanded. Other types of attacks can also be prevented by this. Who can work against any attack, and it will make the proposed secure neighbor construction protocol completer and more comprehensive.

REFERENCES

[1] Elizabeth M. Royer, and Chai-KeongToh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, pp. 46-55, April 1999.

[2] A. Saini and Anu, "Analysis of Security Attacks and Solution on Routing Protocols in MANETs", International Journal of Computer Science and Mobile Computing, vol. 5, 2016 Page: 182-189.

[3] S. Sarika, A. Pravin, A. Vijayakumar and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks", Procedia Computer Science, vol. 92, 2016 Page: 329-335.

[4] ParmarAmisha ,V.B.Vaghelab “Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol” 7th International Conference on Communication, Computing and Virtualization 2016 Procedia Computer Science 2016 Page: 700 – 707.

[5] S. Ji, T. Chen, and S. Zhong. “Wormhole attack detection algorithms in wireless network coding systems”, IEEE Transactions on Mobile Computing, vol. 14,, 2015 Page: 660–674.

[6] M. Hussain and M. Hasan, "Collective Study On Security Threats In MANET", International Journal of Scientific & Technology, vol. 6, 2017 Page: 32-37.

[7] Manish Patel, Akshai Aggarwal, NirbhayChaubey "Wormhole Attacks and Countermeasures in Wireless Sensor Networks: A Survey"International Journal of Engineering and Technology (IJET)Vol 9 No 2 Apr-May 2017 Page:1049-1060.

[8] Ashish Kumar Khare, Dr. J. L. Rana and Dr. R. C. Jain "Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology"I. J. Computer Network and Information Security, 2017, Page: 29-35.

[9] Megha Gupta, Prof. Rakesh Pandit "A Review on Wormhole Detection and Prevention Technique" International Journal of Science, Engineering and Technology Research Volume 7, 2018, Page: 333-336.

[10] P. Balamurugan, K. Marimuthu and M. Shyamala Devi "A Reliable and Efficient Design for Detection ofWormhole Attack in Wireless Sensor Networks" International Journal of Pure and APage:liedMathematicsVolume 119, 2018, 1743-1753.

[11] R. Arun Prakash, W. R. Salem Jeyaseelanand T. Jayasankar "Detection, Prevention and Mitigation of Wormhole Attack in Wireless Adhoc Network by Coordinator" Applied Mathematics & Information Sciences Vol 12, 2018 Page: 233-237.

[12] Abhishek Vyas, Dr. Satheesh A. "Implementing Security Features in MANET Routing Protocols" I. J. Computer Network and Information Security, 2018, Page: 51-57.

[13] Sukhwinder Singh, RajnishKansal "Novel Technique for Detection of Wormhole Attack in MANET" International Journal of Computer Sciences and Engineering Vol.-6,2018 Page: 464-468.

[14] MutumaIchaba "Security Threats and Solutions in Mobile Ad Hoc Networks; AReview"Universal Journal of Communications and Network 6, 2018 Page: 7-17.

[15] Vikram Neerugatti1 and A. Rama Mohan Reddy "Acknowledgement Based Technique for Detection of the Wormhole Attack in RPL Based Internet of Things Networks" Asian Journal of Computer Science and Technology , 2019, Page: 100-104.

[16] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.