ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (223-229), Month: July - September 2020, Available at: www.researchpublish.com

IMPROVING QUALITY OF SERVICE AGAINST WORMHOLE ATTACK BY USING MULTI PATH BASED AODV ROUTING IN WIRELESS AD HOC NETWORK

Sarvesh Kumari[1], Vinita Verma[2], Jagrati Dixit[3], Gajendra Shakya[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]

Sarvesh.chansoliya@gmail.com,jagratidxt@gmail.com

Abstract: **A strategic arrangement of the worm hole can result in an important breakdown in communication across a wireless network. Among of all of these security issues we have considered wormhole attack prevention and detection mechanism in our thesis work. In this thesis, we address the problem of identifying and isolating malicious attack nodes which form wormhole attack. A model is developed for detection and prevention of wormhole, in which have implemented a wormhole detection method based on alternate path. This multi-path technique is based on AODV. And Simulation Analysis show that our implemented approach has good accuracy in terms of PDF and throughput. In simulation have carried out using NS-2 Software.**

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

I. INTRODUCTION

MANET is a collection of mobile nodes that have the ability to communicate with each other without a fixed infrastructure. In this each device is free to move freely in any direction. One of the many benefits of MANETs is that it can be used where there is no proper infrastructure support for wireless access and wired backbones. A major drawback of MANET is that since it is an infrastructure less network that is built on the fly, each node here also acts as a router. Due to constant mobility, rapidly changing topology, decentralized controls, it has to face various security concerns.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.

Security is one of the biggest challenges of MANET. Safety issues in this are mostly concentrated in the safe passage and the parts that install the data transmission safely. And security has become a major concern in wireless networks and has emerged as an important research area. Which are more vulnerable to intrusion by malicious agents than any wired network. MANETs suffer from a variety of security attacks and threats such as: denial of service, flood attack, impersonation attack, selfish node abuse, routing table overflow attack, wormhole attack, black hole attack. Therefore, we have covered one of the important problems in our work wormhole attack.

In this thesis, we have studied and simulated the effects of wormhole attacks. The main objective of this thesis provides wormhole attack prevention and detection mechanisms. A simple scheme based on statistical analysis of multi-paths is proposed to detect such attacks and identify malicious nodes. The proposed multi-path based AODV routing protocol has been analyzed through simulation, and has provided a detailed analysis of the prevention and detection mechanism of the wormhole attack mechanism.

The rest of the paper is organized as follows. In Section 2, we introduce overview of overview of AODV, Section 3 Wormhole attack and NextSections presents aproblem statement and solution model using multipath methodology to prevent a black hole attack, resultand lastly discussed conclusion.

II. OVERVIEW OF AODV ROUTING PROTOCOL

In November 2001, the MANET Working Group published the first version of the AODV routing protocol (ad hoc on demand distance vector) for routing to the IEFT community. AODV belongs to the class of Distance Vector Routing Protocol (DV). Each node in a DV knows its neighbors and the cost of reaching them. A node maintains its routing table, storing all nodes, distances, and next hop for them in the network. If a node is not recoverable, then this distance is set to infinity. Each node periodically sends its entire routing table to its neighbors. So they can check if there is a useful route to another node using this neighbor as the next node, when a link breaks the count-to-infinity. AODV is a protocol run on demand route with a small delay. This means that routes are only established when needed.The protocol consists of two steps:

- Route Discovery.
- Route Maintenance.

ROUTE DISCOVERY: This route discovery process is initiated when a source requires a route to the destination and does not have a route in its route table. To initiate route discovery, the source returns the node in the network to the destination specifying the location along with the RREQ packet. When the node receives the RREQ packet, it checks to see if it is the destination or whether it is the route to the destination. If either case is true, the node creates an RREP packet, which is sent back to the source along the reverse path. Each node with a reverse node sets the forward pointer to the node from which it received the RREP. It travels the way from source to destination. If the node is not the destination and there is no route to the destination, it rebroadcast the RREQ packet. Duplicate RREQ packets are dropped at the intermediate node. When the source node receives the first RREP, it can start sending data to the destination.

ROUTE MAINTENANCE: In this the node detects a broken link when forwarding a packet to the next hop, then it generates a RERR packet that is sent to all sources using the broken link. The RERR packet deletes all routes using a path link. If a source receives the RERR packet and a route to the destination is still required, it starts a new route discovery process. Routes are removed from the routing table if they are not used for a certain time. This is done by the source node and can be divided into: i) the source node runs: the source node starts a new route discovery process, ii or an intermediate node runs: the source node receives a route error message (RERR) Is sent. Intermediate nodes that receive RERR update their routing table by setting the floor distance to infinity. If the source node receives a RERR, it will initiate a new route detection. AODV introduces a local connectivity management to intercept global broadcast messages. This is done by periodic exchanges of so-called halo messages which are small RREP packets with node addresses and additional information [2–5].

III. WORM HOLE ATTACK

The wormhole attack involves malicious nodes located in one area that capture packets and tunnel them to another malicious node located in another area of the network. The wormhole attack involves malicious nodes located in one region that capture packets and tunnel them to another malicious node located in another area of the network. A tunnel has two malicious nodes called a worm hole attack. Attackers use a wormhole in the MANET to make their nodes more attractive so that more traffic can flow through their nodes. During the attack a malicious node grabs packets from one location in the network, and tunnels them to another malicious node at a distant point, which recreates them locally. Once this link is established, attackers can select each other as multiply relays, after which some topology control messages and data packets are exchanged through the wormhole tunnel and the worm hole node is all Drops packets [3].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (223-229), Month: July - September 2020, Available at: www.researchpublish.com

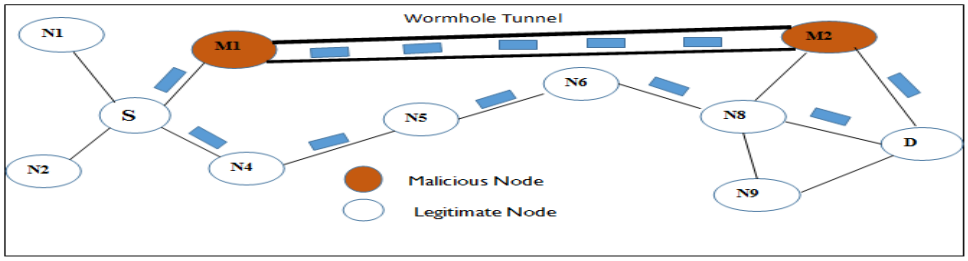


Figure 1: Wormhole attack Problem

The picture depicts the scenario of the wormhole attack. There are two malicious nodes that are far away from each other in the same network or may be in different networks that are connected with each other through a tunnel and pass data packets through the tunnel where they iterate. Occur. In the wormhole attack, the two attackers work together. One receives the packet, tunnels the packet to its partner, and then the partner shows them again to the network. There are two types of wormhole attacks. In the first type, malicious nodes hide the fact that they forward a packet, meaning, legitimate nodes do not know their involvement in packet forwarding. In the second type, legitimate nodes are aware of the fact that malicious nodes are forwarding packets; Just don't know that they are malicious. For the case discussed, we refer to the first type as the hidden attack while the second type as the exposed attack.

After launching a wormhole attack, the attacker has unauthorized access to the given network. Following are the symptoms that can be seen in the network due to wormhole:

- Decrease in Network utility.
- Increase the Traffic Load.
- Increase the Packet Loss.
- Increase Delay.

IV. PROBLEM STATEMENT

MANET is more vulnerable to security attacks by malicious nodes because it does not have a clear defense mechanism. Openness, dynamic and infrastructure-less nature make it prone to security threats. As the biggest security threat of all these attacks, one of the biggest security threats in MANET is the wormhole attack. This is a very damaging attack. These attacks are caused by malicious nodes, so the ad hoc wireless network is vulnerable to malicious node attacks. In which two or more malicious nodes form a virtual tunnel in the network. The main problem is to change the status to a malicious node by tunneling the neighboring node and change the status repeatedly so that it is very harmful to the network. The attacker then modifies the packet address to initiate a data drop using the link break issue.

SOLUTION MODEL: For the last few years, the subject of attack has been the main area of research. In this task, we have found a way to find and resolve a wormhole attack. We prevented the wormhole attack problem by using the algorithm below and performing efficient data transmission. Some modifications have been made to the AODV routing scheme which reduces packet loss. A new protocol known as the multi-path scheme is proposed based on an alternative path to avoid wormhole attack. The proposal technique is used to detect and isolate malicious nodes from the network. The proposed technique is an improvement over existing technology.

Multipath AODV or Modified AODV: Multiple root discovery procedures are used in this scheme, by which multiple routes are discovered. Continuous route breakdown causes intermediate nodes to fall packets because there is no alternate route available to the destination. Therefore, this scheme provides an alternative route for data transfer.

We have modified the AODV algorithm below to correct the wormhole attack:

- In 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 set of the route selector counter should be added for every node in case of one source may have to transmit to more than one destination. The route selector counter is for the source node to switch from the best route to the second route in the next transmission and switch back in the Next Transmission.

VI. SIMULATION PARAMETERS

Simulation Parameters is as follows:

PARAMETERS	VALUE
Simulator	NS-2
Routing protocol	AODV
Number of Nodes	10 to 100
Area	500x500m^2
Packet size	512byte
Simulation time	1000s
Pause time	10.0
Traffic type	CBR
Mac protocol	Mac/802.11
Maximum connection	5
Examined approaches	Normal, With Attack, Without Attack
Speed	10 m/s

VII. PERFORMANCE METRICS

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

Packet Delivery Ratio: This is the Ratio 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.

Average Throughput: Average Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second.

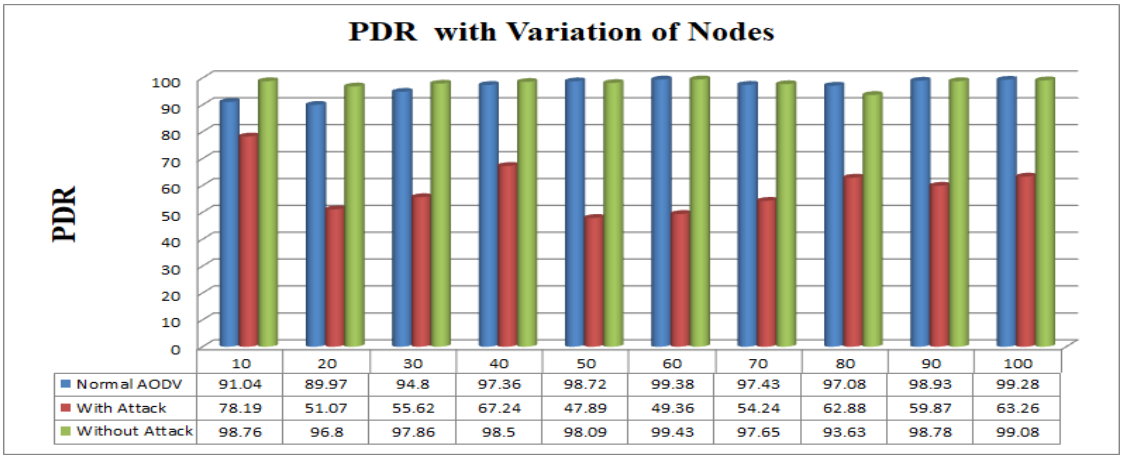
VIII. SIMULATION MODEL

In this section, simulation models of various parameters used in the network scenario were discussed. And the section below gives all the parameters and its values, which are used in our thesis work. To evaluate the network in existence of a malicious node, a wormhole node is created with the help of an agent. A tcl script is created for the implementation, including the creation of nodes, relationships between nodes, setting the topography region in which nodes are located according to the x axis and the y axis. The simulation is run for 1000 seconds. The simulation process was performed for 10 to 100 number nodes. The simulation has randomly distributed nodes in the area of the network's 500x500 m^2 rand function.

IX. SIMULATION RESULT AND DISCUSSION

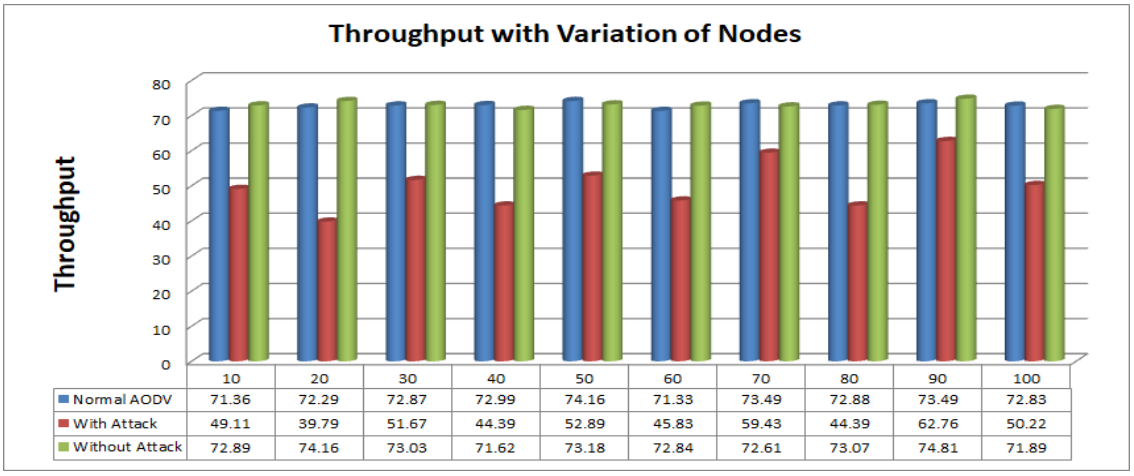
In this thesis, we have found the results with variation of nodes. In figure explain that a malicious node can bring a significant drop in the performance of the network. To study this, simulations have carried out using malicious nodes in a network, to compare it with the normal working of AODV. And also present the performance of the proposed solution that is two types of scenarios are taken into Consideration based on attacks 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.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (223-229), Month: July - September 2020, Available at: www.researchpublish.com



	10	20	30	40	50	60	70	80	90	100
Normal AODV	91.04	89.97	94.8	97.36	98.72	99.38	97.43	97.08	98.93	99.28
With Attack	78.19	51.07	55.62	67.24	47.89	49.36	54.24	62.88	59.87	63.26
Without Attack	98.76	96.8	97.86	98.5	98.09	99.43	97.65	93.63	98.78	99.08

Figure 2: Packet delivery friction with variation of nodes.



	10	20	30	40	50	60	70	80	90	100
Normal AODV	71.36	72.29	72.87	72.99	74.16	71.33	73.49	72.88	73.49	72.83
With Attack	49.11	39.79	51.67	44.39	52.89	45.83	59.43	44.39	62.76	50.22
Without Attack	72.89	74.16	73.03	71.62	73.18	72.84	72.61	73.07	74.81	71.89

Figure 3: Average Throughput with variation of nodes.

Figure-2 and 3 have shownPDR and throughput with variation of nodes. In which are transmitted the Data packets between the source and destination for 10 to 100 nodes successfully. The found the Network Performance with the help of three scenarios. First scenario have found PDR with Normal AODV, in the second scenario we have implemented a wormhole Attack with the help of malicious node and Found PDR for second scenario. In the second scenario we saw that the network performance has decreased due to Attack. Due to this Kind of attack create a link break problem occur, in which the Packet loss increases because the scheme we have used in it follow the single and don't have another Path for Data Transmission. To solve this Problem we have used Multi-Path AODV and with the help of this start data transmission for another route. By the help of Multi-Path AODV control the packet loss and increase the network performance. And finallyit has been observed that modified AODV or Multi-Path Approachhave solved the problem of Attack to a great extent and have enhanced the performance of the network.

X. CONCLUSION & FUTURE WORK

Our thesis report consists of two parts: a theoretical study and a second simulation analysis. The effects of routing attacks on multi-path routing have not been addressed. In this work the performance of multi-path routing under wormhole attack is studied in detail. In the simulation section, a simple multi-path based scheme has detected and identified wormhole attacks and then compared them using a network simulator. To mitigate the problem of malicious packet dropping, we developed a comprehensive abuse detection system in ad hoc networks through a revised scheme, and Results indicates that impact of wormhole attack is affected the network outputs in terms of throughput and PDF. To evaluate the various performance metrics with Attack and without wormhole attack for modified or existing AODV routing scheme, modified AODV works efficient and solve out the malicious node problem. And it has shown the compare results with previous existing research. The investigation shows that the proposed detection techniques can provide improved Throughput and PDF.

Future work:

The wormhole attack involves malicious nodes located in a region that capture the packet causing loss of the packet. And by expanding this proposed model one can consider other types of attacks in future works located in another area of the network. This proposal will make the Secure Routing Protocol compiler 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] P. Chahal, G. Kumar Tak and A. Singh Tomar, "Comparative Analysis of Various Attacks on MANET", International Journal of Computer, vol. 111, 2015 Page: 42-46.

[3] AkanshaShrivastava and Rajni Dubey," Wormhole Attack in Mobile Ad-hoc Network: A Survey" in International Journal of Security and Its Applications Vol.9, 2015 Page: 293-298.

[4] Anal Patel, Nimisha Patel, Rajan Patel "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, 2015 IEEE, 2015.

[5] Samuel Jacob, D DAmbavade, K T V Talele" Performance Evaluation of Wormhole Attack In AODV" Samuel Jacob et al. Int. Journal of Engineering Research and Applications, Vol. 5, Issue 1, 2015, Page: 70-72.

[6] 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.

[7] Swati BhagatandTrishnaPanse "A Review on Detection and Prevention of Wormhole Attack in Wireless Sensor Network" International Journal of Computer Applications, Volume No.13, 2015 Page: 1-4.

[8] Xiaoxia Qi, Qijin Wang and Fan Jiang "Multi-path Routing Improved Protocol in AODV Based on Nodes Energy" International Journal of Future Generation Communication and Networking Vol. 8, 2015.

[9] Reena Shakya, Nitesh Gupta " Prevention and Detection of Wormhole Attack in Mobile Adhoc Network Using Clustering and RTT"IOSR Journal of Computer Engineering Volume 18, 2016 Page: 32-38.

[10] 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.

[11] L. ThangaMariappan, K. Rubasoundar "Isolating Wormhole Attack in Wireless Sensor Networks" International journakof Circuits and Systems scientific research publishing, 2016, Page: 2036-2046.

[12] 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.

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

[14] S. Kumar, M. Goyal, D. Goyal and R. Poonia, "Routing Protocols and Security Issues in MANET" International Conference on Infocom Technologies and Unmanned Systems 2017.

[15] RoshaniVerma, PROF. Roopesh Sharma, Upendra Singh, "New APage:roach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

[16] Pratik Gite, "Link Stability Prediction for Mobile Ad-hoc Network Route Stability", International Conference on Inventive Systems and Control, 2017.

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

[18] PericlePerazzo, Carlo Vallati, Dario Varano, GiusePage:e Anastasi and GianlucaDini_"Implementation of a Wormhole Attack against a RPL Network: Challenges and Effects" 14th Annual Conference on Wireless On-demand Network Systems and Services, 2018 Page: 95-102.

[19] Abhishek Vyas, Dr. Satheesh A. "Implementing Security Features in MANET Routing Protocols" I. J. Computer Network and Information Security, 2018, 8, 51-57

[20] 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.

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

[22] P. Balamurugan, K. Marimuthu and M. Shyamala Devi "A Reliable and Efficient Design for Detection of Wormhole Attack in Wireless Sensor Networks" International Journal of Pure and Applied MathematicsVolume 119 No. 15, 2018, 1743-1753.

[23] 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.

[24] 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 Vol.8 , 2019, Page: 100-104.

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