© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Comprehensive Study of Wormhole Attack in MANETs

Madhu, Rakesh Kumar, Sukhjot Kaur
Sachdeva Engineering College for Girls, Gharuan, Mohali, Punjab, India

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a dynamic network of nodes which are wireless and as well as mobile. It creates a short term or momentary network for the digital and data communication. It has no access point. These days wireless devices are used in high amount so this technology is a governing factor in the success of infrastructure-less mesh. MANET is dealing with active strikes and as well as passive strikes at almost every zone of network model. The flaw in protection parts of their routing protocols is magnetizing a number of assailants to infringe the network. An appropriate kind of intrusion; recognized as Wormhole, which is projected by laying down of tunnels and it's aftereffect in overall break of routing paths on MANET. In this paper a serious investigation is done on warmhole attacks in MANET.

General Terms
Communication, Network, Security Attacks, Nodes

Keywords
MANET, Wormhole, Mobile, Routing.

I. INTRODUCTION

Amid security strikes which are projected in network layer are very serious [10]. The Wormhole strike is one of the most critical security strikes [11] which can crucially reduce the communications across the mesh, it is a network layer strike projected by harmful junctions by creating a passage across which packets are acquired and replayed to other junctions warping the information course and influencing the routing means [9].

II. LITERATURE REVIEW

S Y. Shin et al. [1] proposed an algorithm to notice and segregate wormhole threats in mobile ad hoc networks (MANETs). The prime idea of this research was to generate alternate feasible courses when directing Route Request (RREQ) from origin to target and to operate those paths as instance of each other, in order to establish malicious junctions with mischievous performance inside the mesh.

The algorithm acted in three different strides, which were using routes redundancy, routes aggregation and calculating round-trip time (RTT) of entirely registered routes. Routes redundancy was originated where source forwards RREQ using each feasible route to target. All courses that are joined source and target are registered jointly with the various hops from each route. A few courses assembled in the identical relay point before target was aggregated, so all nodes that joined the mesh can be established and the performance of malicious junctions in could be interrogated. The RTT and various hops of every recorded route were differentiated in order to detect suspicious route. Nodes with suspicious behavior within network were isolated and would not be considered for transmission.

The mesh consisted of 25 junctions where each junction was provided with 802.11 wireless interfaces and established in a square of 2500 x 2500 meters. All junctions in the mesh were operating with arbitrary orientation and joined with everyone. Results showed that when mesh was under wormhole strikes, AODV algorithm demonstrated a notable growth of total packet collapsed up to 430 packets. Former time-based methodology definitely were competent to control the spike enhancement of all packets collapsed up to 200 packets, but the number of packets collapsed still daring than normal condition, which meant wormhole strikers have successfully attack the network. Over said methodology showed the potential to handle the

improvement of total packets collapsed in the strength below 50 packets.

A. Patel et al. [2] had surveyed different methodologies concerning with identification of wormhole strike and an algorithm for wormhole diagnosis and prevention was proposed. Over said methodology was based on the Hash based Compression Function (HCF) which was literally using any secure hash function to compute a value of hash field for RREQ packet.

Source junction S begins route discovery to find target function D. Source junction S begins with Hash based Compression Function (HCF) e.g. SHA-1. Source junction S also begins with Seed Field and cost of Hash Field adjoin it with RREQ and advances it to its adjacent functions. If surrounding functions are equal to target then target function D gets more than one route requests (RREQs) and target D performs HCF, with product of number of hop count with seed cost. In any other way every authenticated medial junction will register HCF on hash field and includes it with RREQ and forward it to its adjacent nodes. If evaluated hashed cost equal to included hashed cost then target D replies RREP (route reply) on way having least hop count. In any other way if evaluated Hashed cost will not comparative to Appended Hashed Value then target D recognizes that RREQ comes from tunnel and adjacent junctions m2 identified as a wormhole striker. Target D adjusts flag = 1 (extra field) in RREP and answers it via tunnel way. Source node S gets RREP with flag=1 and recognized adjacent junction m1 as a wormhole striker.

Theoretical over said methodology judged very favorable equivalent to other clarifications recommended in literature. The over said mechanism would be fused in AODV routing protocol and would be achieved and replicated in NS2.

A. Rana et al. [3] proposed a design to inhibit synergetic intrusions on MANETs. AODV could be continued by summing two categories of control packets and threshold cost: first one is Secure Reliable Route Discovery Request (SRRD_REQ) and second one is Secure Reliable Route Discovery Reply (SRRD_REP). SRRD_REQ messages were also regarded as control packets directed by the source node along with SRRD-ID as target array number of target junction over the MANET on specified periods and SRRD_REP information in feedback of SRRD_REQ by the target to the source junction after coordinating SRRD_ID. SRRD_REP can only be achieved by the target junction as hypothesis which indicates there is no task of other junctions i.e. no node other than the target, can inspire SRRD_REP for the sake of the target node. Moreover, Routing table also holds new fields called Reliability List (RL) and Threshold Value (TV) as routing table record. But no refinement in the arrangement of EMAODV Routing Table access contrast to usual AODV routing table entry besides two supplementary fields RL and TV. RL (Reliability list) holds junctions that are reliable and TV holds mean of every target sequence number of trustworthy junctions.

By utilizing NS2, identical mesh was originated with 23 junctions having a few junctions behave as the Blackhole strike and Grayhole strike identical to rational AODV. The aggrement so constructed amid source and target is UDP. With the assistance of CBR (Constant Bit Ratio) utilization, Traffic was triggered with uniform packets over the UDP connection. Packet area of CBR limited to only 512 bytes and adjusted data rate to 10 Kbps. Similar method is utilized for the simulation of UDP authentication and traffic reproduction in EMAODV as in rational AODV.

This over said was very helpful for 15-45 nodes MANETs for intercepting and diagnosing collaborative strikes black hole and gray hole. But small routing overhead in EMAODV intercepts completed efficiency use of MANET which was not in case of rational AODV. So routing overhead gain speed with gain in MANETs size.

S. B. Geetha et al. [4] proposed a routing methodology was fabricated by gaining the multicast routing aggrements by adding small normal entities e.g. Additional Supportive Beacons (ASR), Route-Discovery Beacons (RDB), and Auxiliary Nodes (AN).

The over said study considered an advanced sort of a junction known as Auxiliary Node (AN), whose primary responsibility was to frequently transmit the Route Discovery Beacons (RDB) incorporated with the size of the amount of operating approaching edges in the proposed routing method. Choice of AN is drifting out

on the ground of greater surplus energy. The ultimate cap of the ASR is set to 3. The over said structure considers that if the volume of the arrival routes were more than the maximum capof ASR than it marked a stage with degraded achievement.

The proposed system updated the multicast cluster data in its AN table as well as table handled by multicast routing in mobile adhoc mesh. The organization than joind, one ASR table for every mobile junction in the chart in direction conserving memory desired in calculation. The arrangement thereby assured insignificant memory convolution.

The outcome highlighted showed that the gain of mobility has no powerful reaction of probability of recognition of tunnel in case of wormhole strike. The system could strongly acquire the recognition of tunnel with the gain of packet capacity and data transmission on immense bandwidth channel. The reaction also showed that voluntary gain in junction velocity was the definite recognition of tunnel.

The cumulative energy exhausted in less than 0.1 Joule. This evidence presented that over said system has better stability of energy confinement of junctions that could be further utilized for the mobile junctions to apply cryptographic algorithms.

S. K. Jangir et al. [5] did a deep study of wormhole attacks in MANET. Wormhole advertised a false shortest path and attracts all the network traffic to it. It had been found that in addition of adding delays in the network, wormhole attacks also decrease the throughput. Different methodologies and techniques utilized for the diagnosis and prevention of wormhole strikes such as packet leashes, directional antennas, time-based mechanisms and many other are considered. A close study had been done on various protocols and attacks in these protocols including OLSR, DSR and AODV protocols. Along with the explanation of these methods we had done qualitative comparison of all the wormhole detection techniques. Overall, a significant amount of work had been done on solving wormhole attack problem.
Author was not sure that this solution is applicable to all situations, but the analysis on various types of wormhole strikes and their diagnosis methods granted in the paper would be useful to frame solid detection technique and a suitable solution for preventing Wormhole attack can be proposed.

H. Ghayvat et al. [6] proposed a preserved path is to diagnose and mitigate wormhole strike. It was achieved Ad hoc on demand distance vector (AODV) methodology which efficiently searchess wormhole strike presented in a MANET and Digital signature is utilized to intercept it. It was a safe approach. It calculated the all over tunneling time taken by tunnel to analyze the behavior of wormhole. After that, it decided static threshold cost. Depending upon this tunneling time and threshold cost it determines whether given junction was wormhole junction or trustworthy junction. Afterward, the digital signature and hash chain algorithm was implemented to counter maliciously (wormhole) junction. It was one of the guarded clarifications because it utilizes Hash function to guard wormhole strike. To diagnose wormhole strike in the over said system, tunneling time logic was utilized. Tunneling time speaks for prevailing situation and region of every junction. In the present scenario, Angle Based methodology was utilized to characterize position and region.

The over said wormhole diagnosis algorithm is executed using network simulator NS2.35. A mesh environment containing of 25 mobile junctions roaming over the simulation area of 1000*1000m with CBR traffic arrangement was followed. This mentioned approach gained lifetime, throughput and reduces network delay of the mobile mesh contrasted to the current system. It administrated QoS up to a good level and elimination of reduntanted errors appeared in the wormhole diagnosis are still open problems.

N. Gupta et al. [7] introduced methodology clarifies and counters the wormhole strikes in a batched adhoc meshes by using the cryptographic methods recognized as the digital signatures. As in the regard of ad hoc meshes there were the clusters and each cluster has their own cluster head CH and there was one CG which performed as the entry amid two clusters which moves or from which the data movess from one cluster to the different cluster. CH was mostly the head of the cluster which analysis the total performance of a appropriate cluster and Cg was the entry junction which acted as the

entry amid the two nodes from which the communication take place amid two clusters or the junctions.

Step 1: One node or junction was elected as the cluster head established on its range or the distance of this junctionss from all the other current junctions. Thus each junction in the cluster was just one hop or leap away from the cluster head and this was the importance of the cluster head to preserve entire these junctions. And therefore complete the performances of one cluster was continued by the cluster head

Step 2: meanwhile one cluster wished to interact with other cluster this could be executed with the assistance of the gateway or entry junctions and it pictured as a boundary amid two concurrent clusters.

Step 3: When individual cluster prepared to handshake with the different cluster it redirected the RREQ from one cluster to the different group to its cluster head to which mentioned RREQ went to the cluster head of the diffferent group through the entry and also RREP is also redirected by the junctions by succeeding this way in the counter arrangement.

Step 4: Besides whole cluster or group head further redirected its public key to total no. of junctions which are commence in its particular cluster. Gateway or entry junctions of the two clusters or groups further had the public keys of their particular groups. And further the public keys of the different clusters to which they were coordinatting with.

Step 5: Whole cluster entry junction acquired two public keys one of its particular and another of the interacting group. Thus, this afore mentioned strategy would not allown this wormhole strike to report as the full operation is experimenting supporting the management of the cluster heads and the gateways and entries were also satisfied in its performance therefore, by which the expectation of mischievous customer to make their individual tunnel reduces to the ultimate achievable degree as an outcome.

The over said protocol accomplishes in countering a wormhole strike as the wormhole way cannot strongly delight the preservance restraints enforced by the digital signatures and also as this arrangement was robust and further very smooth to apply as it did not mendatory appropriate complicated hardware conclusions in it.

C. Gupta et al. [8] presented a way that was efficient to diagnose and counter MANET from the Wormhole strike. For that the frequency and mobability of junctions was investigaed. Individual and all junction within the mesh, desired to help its adjacent, and forth coming hop or next to next hop knowledge.

When source broadcasted RREQ to its adjacent junction for way to target right here authorizing that the mob strength of junctions was less, junctions to search the route, straighway the early infected junction announcement of having recent route to target, then source asks its adjacent, following as good as next to next junction resulting it gathered the proficiency afixed this knowledge in its table, posting packet after some prompts when source not getting conformation from target, it further transmit packet to that route and delaying for inconsistent instantaneous and if as soon as additional no longer getting conformation from target it targets a investigation information packet to that junction adjoning and enquire their adjacent hop and adjancent hop distance and predict to acknowledge from junctions it leads that inspected packet, then it resends that analysed packet to their nearby residents for collecting the information of that particular junction, and replay this strartegy, therefore diagnosing wormhole in MANET on the ground of adjacent hop, next hop distance and nearby residents proficiency. Subsequently observing we introduce this strike by utilizing broadcasting analysed packet to whole junctions as a result junction revises their tables and bar these junctions. In the over said system progress based or adjacent residents based methods gave superior outcome in conditions of the packet delivery proportion, throughput, routing overhead drop, possibility of improvements and upgradations are huge.

A. Khan et al. [9] conferred an approach NWLID: Normalized Wormhole Local Intrusion detection Algorithm that was the updated variation of Local Intrusion Detection Routing Security over mobile adhoc meshes that had an central neighbor junction exploring strucutre, packet drop evaluator, each node receiving packet approximator succeeded by isolation method for the approved Wormhole junctions. During the malicious central junction (node N5) ingested the RREP heading for the source junction (node N1) the earlier junction (node N4) to the central junction operates the process of diagnosis and not the source junction. initially, the last junction offered the RREP packet. Then, it utilized a fresh route to the adjacent junction (node N6) and retransmis FRREQ packet to it. When the earlier junction got the FRREP packet from the adjacent hop

junction, it got the advice from the FRREP packet and performed according to subsequent guidelines: • If the coming junction (N6) had a passage to central junction (N5) and target junction (N7), the earlier hop junction rejected the FRREP, then unicast the RREP to the initial junction.

• If the forth coming hop (N6) had no available passage to the target junction (N7) or the central junction (N5) or both of them (N5 and N7), the earlier junction (N4) rejected the buffered RREP and the FRREP also, at the same instant transmitted the warning report to convey.

It may be the situatin when the junction got the FRREQ report it's a Worm hole junction rather of black hole junction and conveys a mocked FRREP report; in that situation black hole junction came in the mesh, to eradicate that junction in the coordinating mesh, 2nd Normalized stride to be implement for that in the coordinatng FHellow packet format was formated, which was circulated by individual cental junction to consecutive adjacent residents of it coming node, if conveyed by Preclusion Ratio (PR) if PR more than 50%. Individual junction in the coordinating mesh conveyed FHellow Packet to adjancent to its consecutive nearby residents like N2 transmitted to N4 and N3 transmits to N5.

A mesh consisting of 50 mobile junction moving over the simulation area of 1000*1000m with CBR traffic pattern is adopted. Two wormhole tunnels (4 wormhole peers) are considered. The protocol displayed that just one execution of oversaid method could diagnose the movement of wormhole peers. In scenarios of 10,20,30,40 and 50 junctions, the delivery ration of updated AODV was better than regular AODV protocol.

Table 1: Comparison of Various Wormhole Attack Detection Solutions

Papers	Routing Type	Tool Used	Detection Type	Publication Year	Results	Defects	Resource
Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation	AODV	Opnet Modeler	Cooperative	2012	Ability to hold the enhancement of total packets dropped in the stability under 50 packets.	Power consumption and load factor is not discussed	IEEE Int'l Conference on ICTC
Defending Against Wormhole Attack in MANET	AODV	NS2	Cooperative	2015	Algorithm uses Hash based Compression Function (HCF) to compute a value of hash field for RREQ packet.	Theoretical approach not practically implemented	5th IEEE Int'l Conf. on CSNT
EMAODV: Technique to prevent collaborative attacks in MANETs	AODV	NS2	Collaborative	2015	Detect and prevent attacks and packet delivery is highest	Power consumption and load balancing, efficiency is not discussed	Elsevier – 4th Int'l Conf. on ECCS
Elimination of Energy and Communication Tradeoff to Resist Wormhole Attack in MANET	AMRP	MatLab	Cooperative	2015	Detect malicious node on the basis of assumption that normal node can never have increasing velocity as within the increase of simulation time and data forwarding task	Power dissipation is discussed but not efficiency and security of algorithm.	IEEE Int'l Conf. on ERECT
A Comprehensive Review On Detection Of Wormhole Attack In MANET	AODV, DSR, OSLR	NS2, MatLab	Single as well as cooperative	2016	Algorithms are discussed and their pros and cons	Don't provide any solution of problem	IEEE Conf.
Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET	AODV	NS2	Single detection	2016	To detect wormhole attack in the proposed system, tunneling time logic is used	All types of error are not removed	Int'l Conf. on ST
Movement Based or Neighbor Based Tehnique For Preventing	AODV	NS2	Cooperative detection	2016	Packet drop is stable	Efficiency and power dissipation is not discussed	IEEE Int'l Conf on CDAN

III. CONCLUSION

In this review paper different types of wormhole problems are discussed and also the solutions provided by different authors are summarized. So a proper mechanism should be used to avoid wormhole problem in MANETs. In the future work more research papers can be studied to enhance the results of new algorithms.

IV. REFERENCES

[1] Shin S. Y.,(2012) "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation," ICT Convergence, pp. 781- 786.

[2] Patel A. ,Patel N. and Patel R.,(2015) "Defending Against Wormhole Attack in MANET," Fifth International Conference on Communication Systems and Network Technologies, pp. 674- 678.

[3] Rana A. , Rana V. and Gupta S.,(2015) "EMAODV: Technique to prevent collaborative attacks in MANETs," 4th International Conference on Eco-friendly Computing and Communication Systems, pp. 137 – 145.

[4] Geetha S. B. and Patil V. C., (2015)"Elimination of Energy and Communication Tradeoff to Resist Wormhole Attack in MANET," International Conference on Emerging Research in Electronics, Computer Science and Technology, pp. 143-148.

[5] Jangir S. K. and Hemrajani N.,(2017) "A Comprehensive Review On Detection Of Wormhole Attack In MANET ," International Conference on ICT in Business Industry & Government (ICTBIG), pp. 1-8.

[6] Ghayvat H. , Pandya S. , Shah S. , Mukhopadhyay S., Yap M. H. , Wandra, K. H. (2016)"Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET," 10th International Conference on Sensing Technology (ICST), pp. 1-6.

[7] Gupta N. and Singh S. N., (2016)"Wormhole Attacks in MANET," 6th International Conference Cloud System and Big Data Engineering (Confluence), pp. 236- 239.

[8] Gupta C. and Pathak P., (2016)" Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET," 6th International Conference Cloud System and Big Data Engineering (Confluence), pp. 236- 239.

[9] Khan A. ,Richariya V. and Shrivastava S.,(2014) "Normalized Worm-hole Local Intrusion Detection Algorithm," International Conference on Computer Communication and Informatics, pp. 1-6.

[10] Vandana C. P. ,Francis A. and Devaraj S., (2013)"WAD-HLA: Wormhole Attack Detection using Hop Latency and Adjoining node analysis in MANET", International Journal of Advanced Networking and Applications, Volume: 04 Issue: 04.

[11] Vandana C. P. ,Francis A. and Devaraj S.,(2013) "Evalution of impact of wormhole attack on AODV", International Journal of Advanced Networking and Applications, pp. 1652-1656.