View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by E-space: Manchester Metropolitan University's Research Repository

Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET

H.Ghayvat[a], S.Pandya[b], S.V.Shah[b] & M.H.Yap[c]
[a.]SEAT,Massey University, Palmerston North, NZ
[b.]Parul Institute of Engineering and Technology,Limda, India
[c.]Science and Engineering, Manchester, Metropolitan University, UK

***Abstract*—Wireless Communication is an inevitable part of Smart Home domain. A Mobile Ad-Hoc Network (MANET) is defined as an arrangement of wireless mobile nodes which creates a temporary network for the communication. MANET suffers from both kinds of attacks, active and passive attacks at all the layers of the network model. The lacks of security measures of routing protocols allow attackers to intrude the network. Wormhole, the attack is generated by tunnels creation and it results in complete disruption of routing paths on MANET. The proposed security approach is to detect and mitigate wormhole attack. It is secured AODV approach which efficiently finds wormhole attack present in a 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. Afterward, it decides some static threshold value. Based upon this tunneling time and threshold value, it decides whether given node is wormhole node or trustworthy node. A digital signature and hash chain algorithm is applied to mitigate the wormhole node.**

Keywords— AdhocNetworks; MANET Attacks; Wormhole Attack, Tunneling time; Angle Based Scheme; Digital Signature Algorithm component.

I. INTRODUCTION

In an era of prompt advancement in digital technology, most of this technology is focused on proficient monitoring and controlling. Ubiquitously from mammoth structure building automation to a smart small home, big industrial assembly mechanisms to the tiny toy, an ordinary undergraduate laboratory to international space research center and even health care service at a desk through wireless sensor & networks, and WSN has become an indispensable and crucial device in playing an important role. The main research problem is how to provide security protection to the network topology and the routing in a MANET. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control [1, 2, 14].

Some of the wireless sensing applications run in vulnerable environments which require secure communication and routing such as, Military Arena, Provincial level, Personal Area Network, Bluetooth and Commercial Sector etc.[13]. There are some concerns related to Quality of Service (QoS), security, scalability, power control and performance measurement of MANET [16].

There are two different kinds of attacks in MANET, external and internal attacks. (a) External Attack: These attacks are carried out by nodes that do not belong to the network. It causes congestion and sends false routing information. It also causes unavailability of services. (b) Internal Attack: These attacks occurred from the nodes that are part of the network. In this attack, the malicious node gains unauthorized access and pretend as a genuine node. Wormhole attack, blackhole attack, grey hole attack, flooding, replay attack, DoS(Denial of Service) attack, Man-in-middle attack and evasdroping attack[16] are different types of attacks form in MANET and create trouble in network topology which troubles upper layer Applications.

Fig.1 shows the wormhole attack. At one end of the tunnel, a malicious node captures a control packet and sends it to another collaborating node at the other end through a private channel, which rebroadcasts the packet locally. There are mainly two phases which describe working on wormhole attack. In the first phase, the wormhole nodes involved themselves in several routes [6, 11,12]. In the last phase, these malicious nodes start exploiting the packets they receive. These nodes can confuse the protocols that depend on upon location or geographic proximity of nodes or the colluding nodes may forward data packets back and forth to each other in case of the virtual tunnel so as to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes [8,10].

II. RELATED WORK

Normalized Wormhole Local Intrusion detection Algorithm is the modification of Local Intrusion Detection Routing Security MANET. It has an intermediate neighbor node discovery mechanism, packet drop calculator, individual node receiving packet estimator followed by isolation technique for the confirmed Wormhole nodes [3].

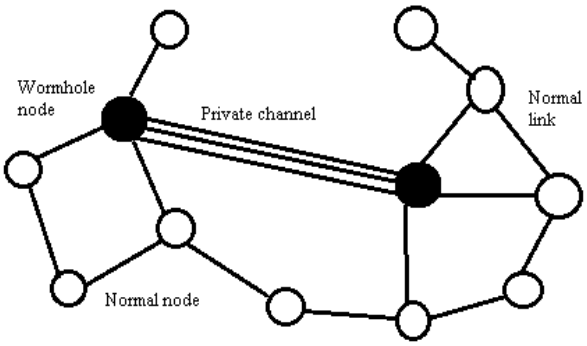

Figure 1: Wormhole attack

Neighbor node analysis is an approach to providing a solution for secure transmission in MANET and to identify wormhole attack and removes wormhole link in MANET[7]. The approach is based on per-hop latency determination and adjoining node (intermediate node) detection techniques which describe the approach of encapsulating the packets in AODV routing protocol. All the packets are encapsulated/decapsulated by the wormhole peers, creating a wormhole tunnel or link[11]. The proposal for using RTT estimator based wormhole detection mechanism was to identify wormhole tunneling attack in MANET which works efficiently and detect all the wormhole suspicious activity [4]. A General mechanism, it can be used without hardware. It describes detection packet which contains location information and clock synchronization for detecting malicious node in MANET. Detection Packet has three fields: processing bit, count to reach next hop and time stamp [15].

III. METHODOLOGY

The proposed system is a security approach to detect and mitigate wormhole attack. It is secured AODV approach which efficiently finds wormhole attack present in a MANET and prevents it from using Digital Signature. It calculates the all over tunneling time taken by tunnel to analyze the behavior of wormhole. After that, it decides static threshold value. Based upon this tunneling time and threshold value it decides whether given node is wormhole node or trustworthy node. Afterward, the digital signature and hash chain algorithm is applied to prevent maliciously (wormhole) node. It is one of the secured solutions because it uses Hash function to prevent wormhole attack. To detect wormhole attack in the proposed system, tunneling time logic is used. Tunneling time represents current position and location of every node. In the present system, Angle Based Technique is used to describe position and location. Tunneling time can be presented as:

Tunneling time=tunnel second+(l/c)-ETX…… (1)

Where,
Tunnel second=How much time tunnel take place,
I=speed of transmission,
c=speed of light,
ETX=transmission power

The Wormhole detection and Advance AODV approach are implemented in following steps:

- Step 1: Source Initialization: Initialize source in MANET using AODV protocol.

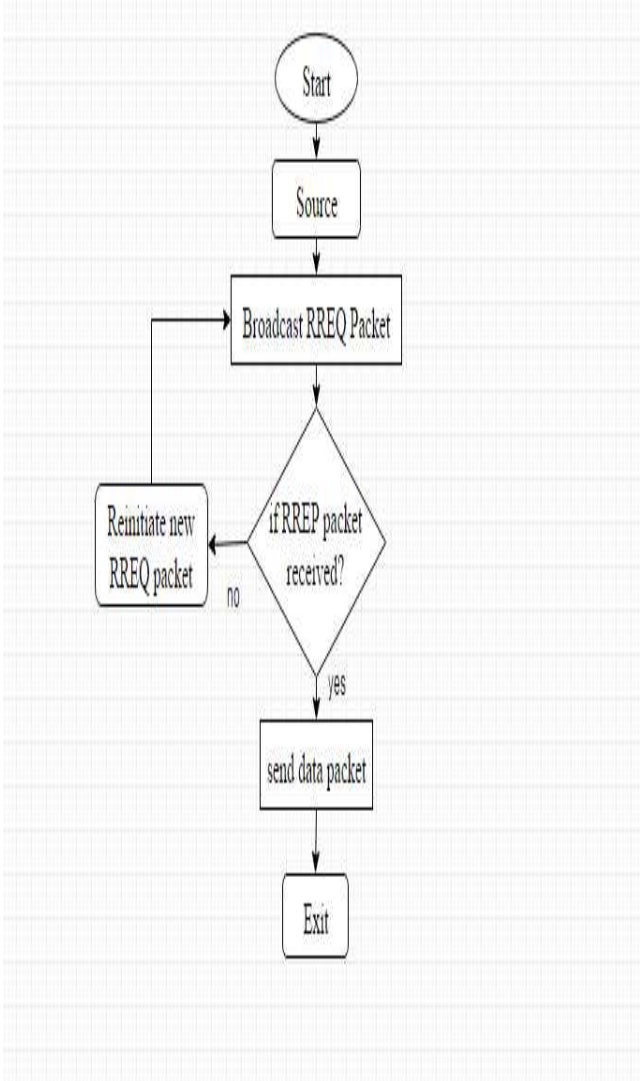

Figure 2: Source Initialization

- Step 2: Detection of wormhole attack takes place based on the following flowchart:

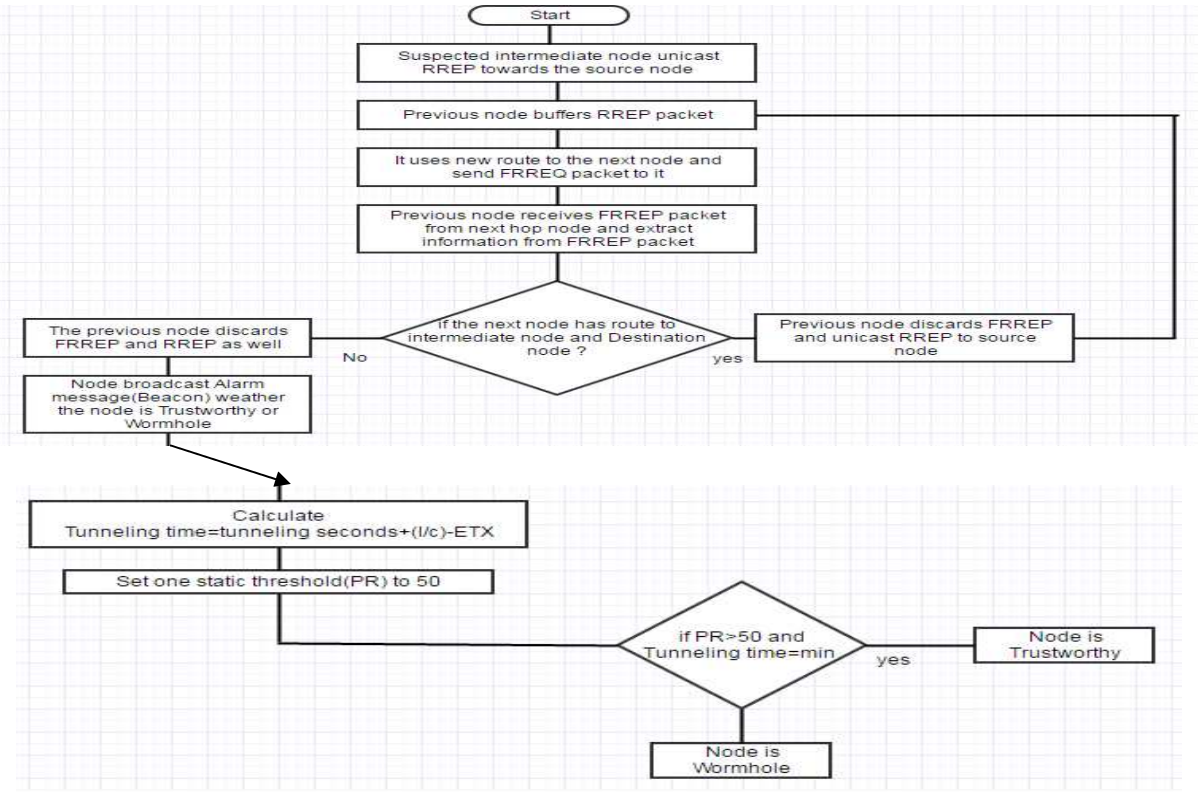

Figure 3: Detection of wormhole Attack

- Step 3: Prevention of Wormhole Attack:

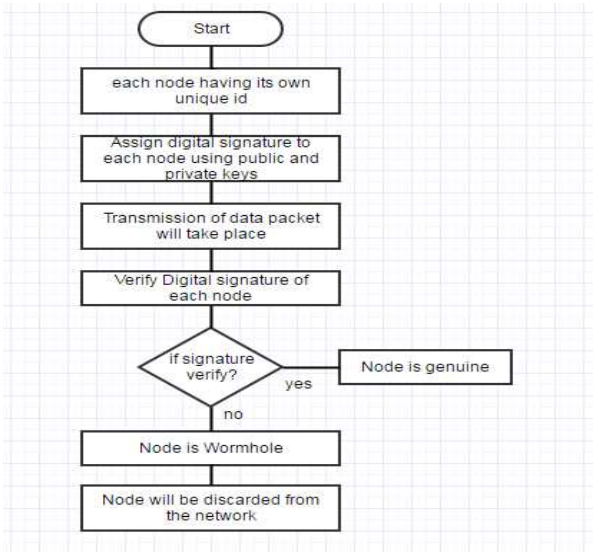

Figure 4: Prevention of Wormhole Attack

IV. SIMULATION SETUP AND RESULT-ANALYSIS

The proposed wormhole detection approach is simulated using network simulator NS2.35. A network environment consisting of 25 mobile nodes roaming over the simulation area of 1000*1000m with CBR traffic pattern is adopted. Two wormhole tunnels (4 wormhole peers) are considered. Simulation parameters are shown in Table.I.

Table I: Simulation Parameters

PARAMETER	VALUE
Area	1000m*1000m
Simulation Time	200 sec
No. Of Nodes	25
Traffic Model	CBR
Mobility Model	Random Way Point
Routing Protocol	AODV
Transmission Range	250m
No. Of Network Connection	1/2/3
MAC Protocol	802.11
Packet Size	512

Fig.5 shows the average network delay comparison among Attack, AODV, NWLIDA and SAODV approach. Fig.6 shows throughput, fig.7 shows packet delivery ratio among Attack, AODV, NWLIDA, and SAODV approach. Fig.8 shows the digital signature technique to prevent the wormhole attack.

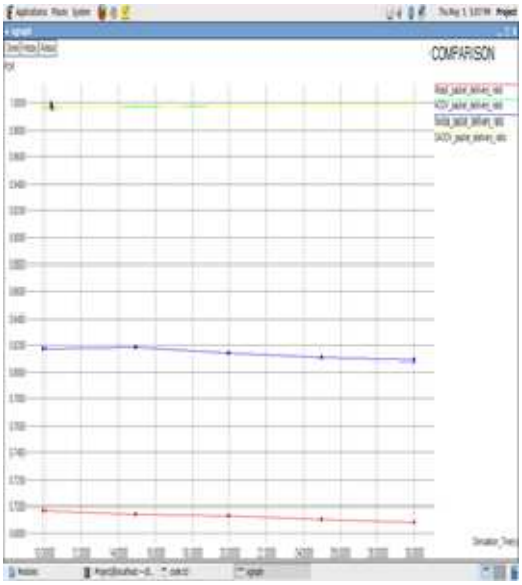

Figure 5: End-to-End Delay Comparison

Figure 6: Digital Signature technique to prevent wormhole Attack

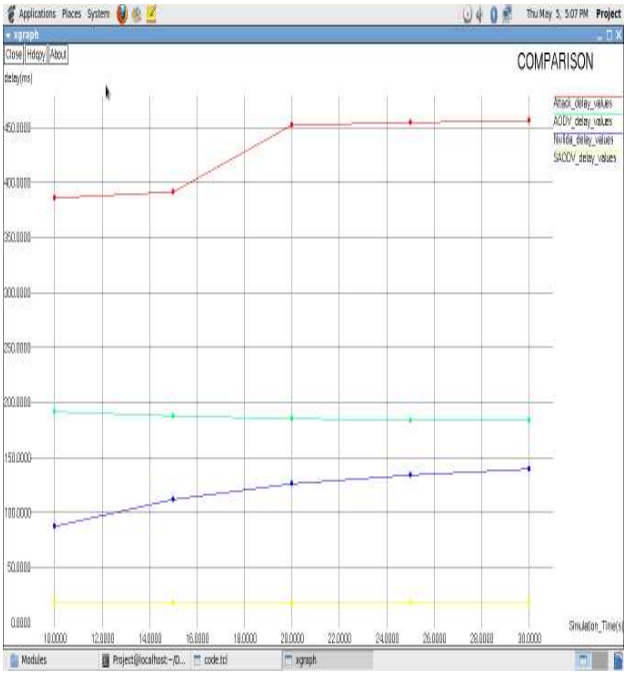

Figure 7: PDR Comparison

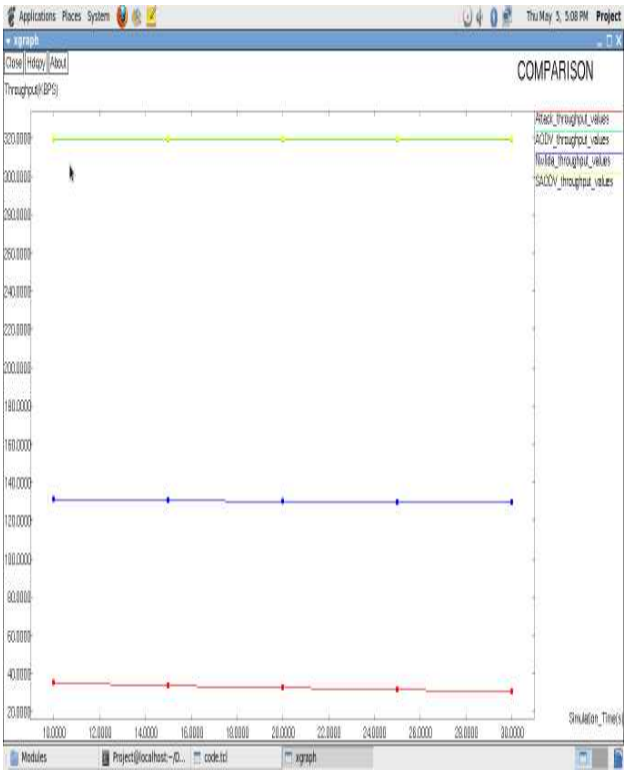

Figure 8: Throughput Comparison

V. CONCLUSION

The existing systems do not calculate the processing time taken by tunnel to analyze the behavior of the wormhole. The proposed scheme is calculating the processing time of tunnel. This proposed approach increases lifetime, throughput and minimizes network delay of the mobile network compared to the existing system. It provides QoS up to a satisfactory level and removal of unwanted errors occurs in the wormhole detection are still open issues.

VI. REFERENCES

[1] Anal Patel, Nimisha Patel, Rajan Patel "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technology, 2015, Gwalior, 4-6 April 2016, pp.674-678.

[2] Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala, Muhammad Hanif Durada "Analysis of Detection Features for Wormhole Attacks in MANETs", Procedia Computer Science vol.56, 2015, pp.384 – 390.

[3] Aarfa Khan, Prof. Shweta Shrivastava, Prof. Vineet Richariya "Normalized Wormhole Local Intrusion Detection Algorithm(NWLIDA)", International Conference on Computer Communication and Informatics, 2014, Coimbatore, 3-5 Jan 2014, pp.1-6.

[4] Neha Agrawal,Nitin Mishra "RTT based Wormhole Detection using NS-3", Sixth International Conference on Computational Intelligence and Communication Networks, Bhopal, 14-16 Nov 2014, pp.861-866.

[5] Ms Neha Choudhary, Dr Sudhir Agrawal "Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – volume1 issue10, Dec 2014, pp.1-6

[6] Devendra Singh Kushwaha, Ashish Khare, J. L .Rana "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 62– No.7, January 2013, pp.21-25

[7] Sweety Goyal, Harish Rohil, "Securing MANET against Wormhole Attack using Neighbor Node Analysis", International Journal of Computer Applications (0975 – 8887) Volume 81, Issue 18, November 2013, pp.44-48.

[8] Yashpalsinh Gohil, Sumegha Sakhreliya, Sumitra Menaria "A Review On: Detection and Prevention of Wormhole Attacks in MANET", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013, pp.1-6.

[9] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", Third International Conference on Advanced Computing & Communication Technologies, Rohtak, 6-7 April 2013, 288-292

[10] Vikaskumar Upadhyay,Rajesh Shukla "An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats", Int. J. Advanced Networking and Applications , Volume 05, Issue01,2013, pp.1858-1866

[11] Vandana C. P, Dr. A. Francis Saviour Devaraj "WAD-HLA: Wormhole Attack Detection Using Hop Latency And Adjoining Node Analysis In MANET", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March – 2013, pp.1-6

[12] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", ISBN 978-1-4614-1405-6 ,DOI 10.1007/978-1-4614-1406-3, © Springer Science+Business Media, LLC 2012

[13] D. Helen, D. Arivazhagan "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014, pp.453-457

[14] Nidhi Nigam,Vishal Sharma,Mahesh Malviya "A Novel Approach for Wormhole Detection in MANET", International Journal of Computer Applications (0975 – 8887) Volume 63– No.7, February 2013, pp.6-11

[15] Priyank Nayak, Akshay Sahay, Yogadhar Pandey"Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013, pp.1216-1222

[16] Priyanka Goyal, Vinti Parmar, Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, pp.32-37

[17] Sopan W.Bagalkar, S. B.Rathod "A Technique of Using Digital Signature Network clustering to prevent from wormhole attack", IJCAT-International Jornal Of Computing and Technology, Volume 2, Issue 6, June 2015, pp.190-195.