Advances and Applications in Mathematical Sciences
Volume 20, Issue 2, December 2020, Pages 331-344

A REVIEW OF PROPOSED SOLUTIONS FOR WORMHOLE ATTACK IN MANET

NISHA SHARMA, MANISH SHARMA and D.P. SHARMA

Research Scholar, SGVU
Jaipur, Rajasthan, India
E-mail: sharma_nisha2005@rediffmail.com

Associate Professor, HOD, CSIT, SGVU
Jaipur, Rajasthan, India
E-mail: manish.sharma@mygyanvihar.com

Principal, MAISM
Jaipur, Rajasthan, India
E-mail: dp.shiv08@gmail.com

Abstract

All around the world, majority of people depends upon wireless adhoc network. So it becomes the most priority to reduce the vulnerability of Wireless network. Wireless networks are exposed to many different types of attacks out of which wormhole attack is most dangerous. Unlike many other attacks on ad hoc routing, wormhole attack is very powerful and cannot be prevented with cryptographic means because intruders does not modify the packet data ,it simply replays the packets. A strategic placement of the wormhole can result in a significant breakdown in communication. In this paper, study of some existing techniques for detection and prevention of wormhole attack is presented.

Introduction

Ad hoc means "for this specific purpose". Ad hoc network is a paradigm of networks which allows nodes unrestricted mobility with no underlying infrastructure. In ad hoc network autonomous nodes form a multi-hop radio network for communicating with each other and maintain connectivity in a

2010 Mathematics Subject Classification: 68M10, 94A60.

Keywords: Ad-Hoc Network, Wormhole attack, Tunneling, Malicious nodes, counter measures.

Received April 15, 2020; Accepted July 20, 2020

decentralized manner. Each node operates as both a host and a router. In other words ad hoc network is based on dynamic topology, because the nodes are mobile and keep changing connectivity among nodes with time. Wireless ad hoc networks can be classified in 3 forms mainly as shown in the Fig. 1 In this paper; our discussion will mainly focus on the MANETs. Significant applications of MANETs include as follows:

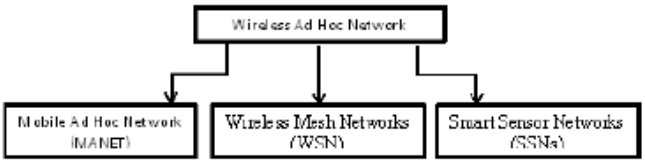

Figure 1. Classification of Wireless Ad Hoc Network.

1. Tactical Network : Military communication, Automated battlefields

2. Emergency Services : Search and Rescue operations, Policing and Fire Fighting

3. Educational : Virtual classrooms, Conference rooms, Sport Stadium and Library

4. Home and Entertainment: Home/Office wireless networking, Personal Area network, Cellphone, ear phone, wrist watch), Multiuser games, Outdoor internet access.

Increasing use of ad hoc network introducing new security challenges. The ad hoc networks are usually more susceptible to physical security threats. The possibility of denial-of-service, eavesdropping, spoofing and impersonation attacks increases [1]. Like infrastructure based networks, the ad hoc networks security is also measured in terms of availability, authentication, confidentiality, integrity, non-repudiation, access control and usage control [2, 3]. But security methodologies used for the fixed networks are not feasible for Ad hoc networks due to its salient characteristics. However, traditional cryptographic solution is inadequate against threats from internal malicious nodes [4].

This paper presents a study on wormhole attack and its countermeasures in Mobile Ad hoc Networks (MANET) with their future

scope. The paper is organized as follows: Section II gives an overview of wormhole attack in ad hoc networks. Section III presents review on some existing wormhole detection and prevention schemes. In section IV, shows the future scope of wormhole detection and prevention schemes discussed earlier. Finally, the conclusions are given in the last section.

II. Wormhole Attack

The growing popularity and usage of wireless technology is creating a need for more secure wireless adhoc network. A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad hoc networks. In this attack, a malicious node captures packets from one location in the network and "tunnels" them to another malicious node at a distant point which replays them locally. The tunnel can be established in many ways e.g. inband and out-of-band channel. This makes the tunneled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc. Wormhole can be formed using, first, in-band channel where malicious node M1 tunnels the received RREQ (route request) packet to another malicious node M2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between M1 and M2. Second, out-ofband channel where two malicious nodes M1 and M2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in Figure 2.

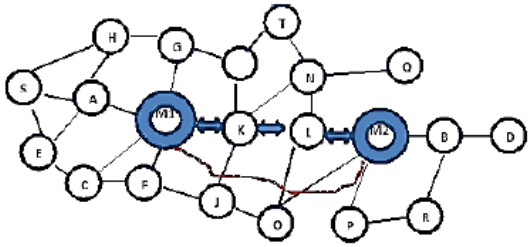

Figure 2. Wormhole Attack.

When malicious nodes form a wormhole, they can reveal themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack [5], while the latter is a hidden or close one. In Figure 2, the destination D notice that a packet from the source S is transferred through node A and B under hidden wormhole attack, while it believes that the packet is delivered via node A, M1, M2, and B under exposed wormhole attack.

Wormhole Detection and Prevention Techniques

Detection and Prevention of wormhole has been an active area of research for past few years. In this section we are discussing some of the existing techniques, their pros and cons. The methods are discussed in the sequence as they came into existence to overcome the limitations of previous method.

1. Y. C. Hu, A. Perrig, and D. B. Johnson [2003] presented a general mechanism, called packet leashes, for detecting and defending from wormhole attacks, and a specific protocol, called TIK, that implements leashes [6.]. In this mechanism information is attached in the packet to limit the transmission distance of the packet so as to avoid tunneling. The authors named the information as packet leash and proposed two types of packet leashes: temporal and geographical leashes. In geographical leashes, location information of node in the network and secure synchronized clock together verify the neighbor relation. In temporal leashes, the packet transmission distance is calculated as the product of signal propagation time and speed of light. Geographical leashes are more advantageous than temporal leashes as they do not require a tightly synchronized clock. It has the limitations of GPS technology.

2. S. Capkun, L. Buttyan, and J. Hubaux [2003], presented mechanism SECTOR [7.]. SECTOR method uses Mutual Authentication with Distance-bounding (MAD) protocol for the estimation of distance between 2 nodes or users. MAD operates in the assumption that every node is equipped with transceiver as extra Hardware. It accepts a single bit, carry out 2-bit XOR process over it and broadcast it. This proposed mechanism, due to their efficiency and simplicity, is compliant with the limited resources of most mobile devices. It is also able to adapt the protocols to the specific needs of a

given application. The overhead is very reasonable, and the mechanism is robust with respect to attackers of different degrees of strength. This paper addresses the problem of securing topology and encounter tracking; the only exception is the prevention of the wormhole attack.

3. L. Hu and D. Evan [2004], The author employed directional antenna to find and prevent the wormhole attack [8]. In this method the directional information is shared between source and destination to estimate the direction of received signal and angle of arrival. Two nodes are communicating with one another, they receive signal at opposite angle. The technique is assumed that nodes maintain correct sets of their neighbors. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are neglected. However this theme is unsuccessful only if the attacker placed wormholes residing between two directional antennas.

4. Issa Khalil, Saurabh Bagchi, and Ness B. Shroff [2005] developed Secure Neighbor Discovery and Monitoring Based approach called LITEWORP: Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network [9]. The position of each node in the network is traced by central authority and it is capable of even isolating the malicious nodes globally. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbors. While in a standard ad hoc routing protocol node usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors‟ neighbors are. After authentication, nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors‟ behavior to determine whether data packets are being properly forwarded by the neighbor, so called „watchdog‟ approach. In LiteWorp nodes not only verify that all packets are forwarded properly, but also make sure that no node is sending packets it did not receive. Since node's neighbors are determined and detected only once in LiteWorp, and the packets from non-neighboring nodes are rejected, no node movement is allowable. Therefore, LiteWorp is applicable to static networks only. The detection rate of this method decreases as the network mobility increases.

5. Chiu, HS; Wong Lui, K.S. [2006] suggested DelPHI (Delay per Hop

Indication) technique that provides a solution to the exposed wormhole attacks [10]. In this mechanism, delay per hop is determined in every path and it is proved that delay per hop for the genuine path is shorter than the wormhole path. If the path has noticeably high delay per hop, then the corresponding path is affected by wormhole. The advantage of DelPHI is that it does not require the mobile node equipped with some special hardware, which in turn provide higher power efficiency. It can detect both hidden and exposed attack but cannot pin point the location of wormhole attack.

6. Jakob Eriksson, Srikanth V. Krishnamurthy, and Michalis Faloutsos [2006] deployed TrueLink: A wormhole detection technique that depends on time-based mechanisms [11]. TrueLink verifies whether there is a direct link for a node to its adjacent neighbor. Wormhole detection using TrueLink involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

7. P. Van Tran, L. X. Hung, Y. K. Lee, S. Lee, and H. Lee [2007] proposed a transmission time-based mechanism (TTM) to detect wormhole attacks [12]. TTM detects wormhole attacks during route setup procedure by computing transmission time between every two successive nodes along the established path. Wormhole is identified base on the fact that transmission time between two fake neighbors created by wormhole is considerably higher than that between two real neighbors which are within radio range of each other. TTM has good performance, little overhead and no special hardware required. The limitation of this scheme is that it is designed specifically for

Ad Hoc On-Demand Vector Routing Protocol (AODV).

8. Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava [2009], suggested Topological Technique [13]. Normally, a wireless multi hop network is deployed on the surface of a geometric environment, such as a plane or a rough terrain. In this method author developed principles in continuous domain, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping to the points on the surface to detect wormhole nodes. A new topology space is formed after the wormhole is glued on the original surface. The Author subsequently analyses how the different topology spaces are generated after gluing different types of wormholes. Author classified wormholes into four categories, according to their topological impacts:

a. Class I wormhole, both of its two endpoints locate inside the surface.

b. Class II wormhole has one endpoint inside the surface and the other on the boundary of the surface.

c. Class III wormhole has its endpoints on two different boundaries.

d. Class IV wormhole has both of its endpoints on the same boundary.

The four types of wormholes have different topological impacts on the original surface, and the complex wormhole attack can be considered as a finite combination of them. Base on their effect on topology, detection of wormhole can be done in the topology.

9. Shalini Jain and Dr. Satbir Jain [2010] In this paper presents a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means [14.]. In this scheme, trust levels in neighboring nodes based upon their sincerity in execution of the routing protocol is derived. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes. The routes established in this manner may not be the shortest in terms of number of hops but will be trustworthy. This scheme functions effectively in the presence of wormhole attack and does not impose any unnecessary conditions upon network establishment and operation phase. The drawback of the scheme is it works only when tunneling of packets is done above the network layer.

10. Saurabh Gupta, Subrat Kar, S Dharmaraja [2011] developed an algorithm called WHOP: Wormhole Attack Detection Protocol using Hound Packets [15.]. After the route discovery, source node initiates wormhole detection process in the established path which counts hop difference between the neighbors of the one hop away nodes in the route. In this a protocol for detecting wormhole attacks without use of any special hardware such as directional antenna and precise synchronized clock and the protocol is also independent of physical medium of wireless network and also efficient in detecting wormhole of large tunnel lengths.

11. Juhi Biswas, Ajay Gupta, Dayashankar Singh [2014], in this paper, AODV routing protocol is modified in order to detect and prevent wormhole attack in real world MANET and Wormhole Attack Detection and Prevention Algorithm (WADP) is implemented on this modified AODV [16.]. In order to detect malicious nodes in the network and to remove false positive problem node authentication mechanism is used. Moreover, simulation results show that node authentication not only removes false positive but also helps in mapping exact location of wormhole and is a kind of double verification for wormhole attack detection. This algorithm does not use any special hardware for detecting wormhole attack.

12. Dhruvi Sharma, Vimal Kumar, Rakesh Kumar [2015], In this paper, an identity-based signature scheme along with clusters is proposed for protecting network from wormhole attack [17]. Cluster based architecture is used in which cluster heads are chosen in such a way that they cannot be malicious. The proposed scheme operates in three phases namely Setup phase, Communication phase and secure data transfer phase. This scheme does not need to distribute any certificate among nodes, so it reduces computation overhead. Simulation results show the improved performance of proposed scheme in terms of throughput, packet delivery ratio and end-to-end delay. Drawback of this technique is it protects wormhole attack that are launched by packet replay only.

13. Chitra Gupta, et al. [2016], In this paper, author believes that MANET routing protocols must have reactive, anonymous and stateless etc properties according to the results achieved from previous methods [18]. Author proposed a Movement based and Neighbor based technique based on various parameters such as routing overhead drop, packet delivery ratio, throughput. For sudden enhancement in the network more network

parameters are assessed also prevents various other types of probable network layer attacks from entering in the network. Further, the proposed mechanism can be improved in future by adjusting mobility and dynamic algorithm parameters.

14. ElhamZamani and Mohammadreza Soltanaghaei [2016], in this paper, authors present a new protocol named M-AODV [19.]. The proposed protocol is based on overhearing the neighbors and constant comparison of the information of main and alternative tables and proposed protocol is found to be safe and some attacks are tested on it. Wormhole attack is detected by overhearing the nodes. The results show that M-AODV has been improved in terms of packet delivery ratio, and the delay has been reduced as well, but the amount of overhead had been increased. M-AODV also improves the quality and security of networks. When security measures are taken, the proposed method has attributes such as overhearing, immediate updating, local repair, and two routing tables. It is assumed that the proposed protocol may act like some other secure methods, such as neighbor overhearing (NEVO) and Packet Travel Time (PTT), which have some of these features as well and may be secure against some attacks. Thus, in simulations, the proposed protocol is proved to be secure against wormhole and black hole attacks.

15. H.Ghayvat, et.al [2016], The wormhole attack within MANETs can be efficiently identified with the help of this Advanced Ad hoc on demand distance vector (AAODV) technique [20.]. For the prevention of this attack, digital signature is utilized here. The decision whether the given node is genuine, or wormhole node can be made on the basis of calculated tunneling time and threshold value. For the mitigation of wormhole node, the digital signature as well as hash chain algorithm is applied. In comparison to the existing approach, the lifetime, and throughput of proposed technique are maximized and the network delay is reduced here. The QoS is enhanced here using proposed approach however, the still concerning issue is the elimination of unwanted errors.

16. Supriya Khobragade, Puja Padiya [2016] The Authors proposed an efficient Wormhole attack detection and prevention method called Wormhole Attack Prevention and Detection Using Authentication Based Delay per Hop Technique for Wireless Network [21.]. Detection of wormhole attack is done using number of hops and delay of each node in different paths available in

network from source to destination and vice versa. The sender node is capable to identify both types of wormhole attacks, in band and out of band. Proposed technique detects the legitimate path and isolates the path under the wormhole attack. This technique does not require any special hardware.

17. Roshani Verma, et al. [2017] the main of this paper is the identification and elimination of wormhole attack during the transmission and propagation processes [22]. The security of ad hoc networks is enhanced by this proposed algorithm. The system considers on Hop technique, where each packet requires transmission over a single link. For identifying the wormhole nodes at high speed, the table entries at destination node are enhanced here. The novel approach also helps in deployment of efficient methods through which the DoS attacks and hybrid attacks can also be prevented from enter the networks such that their security is improved. The packet delivery ratio is increased, and the control overhead is minimized through the enhancement of routing protocols in the networks.

18. Mohammad Rmayti, Lyes Khoukhi [2018] proposed a graph based scheme for wormhole attack detection in MANET. This paper is based on the fact that the Wormhole tunnel reduces significantly the length of the paths passing through it [23]. This solution requires no special hardware, such as GPS, and no clock synchronization. It is based only on the information exchanged between different nodes also the routing table of neighboring nodes. The problem here is that it is able to detect encapsulation type wormholes only and it cannot detect when the wormhole path length is equal to or less than 4 hops. The method assumes network to be homogeneous and symmetric.

19. Sayan Majumdar, Prof. Dr. Debika Bhattacharyya [2018] The Authors proposed Absolute Deviation Covariance and Absolute Deviation Correlation algorithms to detect Wormhole in MANET [24.]. The algorithm detects Wormhole by calculating Correlation coefficient between packet sent and packet received. If the correlation coefficient between packet send and packet received is high, the node is malicious. Further, the Absolute Deviation Correlation Coefficient is utilized to identify the wormholes by measuring the packet drop pattern. The proposed algorithm does not require any extra conditions for its execution, also it is light weight and robust. The

disadvantage of this method is it increases computational complexity and it also requires additional information to be known in prior.

Research Scope

After studying above mentioned existing techniques for Wormhole Detection and Prevention in mobile ad hoc network, observed that these methods have some limitations which open door for further research. The Future scopes for some of the techniques are summarized in table 1.

Technique	Limitations/Future Scope
Packet leashes : Geographical and Temporal (TIK Protocol)	Special hardware like GPS and extremely Synchronized Clock is required works only for detecting physical layer wormhole attacks.
SECTOR	This Technique assumes that every node is equipped with transceiver as extra Hardware
Directional Antenna	Unsuccessful only if the attacker placed wormholes residing between two directional antennas.
LITEWORP (Lightweight Countermeasure for the Wormhole Attack)	Its works only for static type of network.
DELPHI (Delay Per Hop Indication)	Not able to pin point the location of wormhole attack.
TTM (Transmission Time-Based Mechnism)	Works only for Ad Hoc On-Demand Vector Routing Protocol (AODV)
Trust based scheme	It works only when tunneling of packets is done above the network layer
WHOP: Wormhole Attack Detection Protocol using Hound Packets	Process Delay time is more

Identity-based signature and cluster based scheme	protects wormhole attack that are launched by packet replay only
Movement and neighbor based technique	This method consider various parameters except mobility and dynamic algorithmic parameters
Advanced AODV Approach	occurrence of unwanted errors
TrueLink	Need Synchronized clock and works only for hidden attacks
New Approach by Roshini	Need improvement in table entries at destination node to get the detection of wormhole nodes faster application of this approach for DOS and Hybrid attack
Graph based Method by Rmayti	It works for homogeneous and symmetric type of networks
Absolute Deviation Statistical Approach	Computational complexity and requires information in advance

Conclusion

It seems challenging to provide a general security solution for the mobile ad hoc networks. The discussed solutions are implemented based upon different criteria such as using special hardware, protocol modification, using extra nodes for monitoring the network traffic etc. Each scheme has its own strengths and weaknesses. The protocol modification may have extra overhead or cause delay in the route discovery process. The use of special hardware can be expensive or resource starving. And many techniques utilized the end-to-end delay calculation to detect the wormhole link, but it is not an appropriate feature for the wormhole detection. The use of extra nodes can increase the deployment cost. Traditional cryptographic solution is not appropriate for the new paradigm of the networks. As can be seen from the above analysis, what is lacked in the ad hoc networks is trust since each node must not trust any other node immediately. If the trust relationship among the network nodes is available for every node, it will be much easier

to select proper security measure to establish the required protection. It will be wiser to avoid the un-trusted nodes as routers. Moreover, it will be more sensible to reject or ignore hostile service requests. Therefore, the trust evaluation becomes a before-security issue in the ad hoc networks. The security solution should be dynamic based on the changed trust relationship.

References

[1] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF RFC2501, 1999.

[2] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network, 13(6) (1999), 24-30.

[3] Yongguang Zhang and Wenke Lee, Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.

[4] Hong Mei Deng, Wei Li and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE Communications Magazine (2002), 70-75.

[5] Y. Gohil, S. Sakhreliya and S. Menaria, A Review On: Detection and Prevention of Wormhole Attacks in MANET, International Journal of Scientific and Research Publications 3(2), 1 ISSN 2250-3153, February 2013.

[6] Y. C. Hu, A. Perrig and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in Proc. INFOCOM 3 (2003), 1976-1987.

[7] S. Capkun, L. Buttyan and J. P. Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks, in Proc. First ACM Workshop on Security of Ad Hoc and Sensor Networks (2003), 21-32.

[8] L. Hu and D. Evan, Using Directional Antennas to Prevent Wormhole Attacks, In Network and Distributed System Security Symposium, San Diego, California, USA,2004.

[9] S. Khalil, Bagchi and N. B. Shroff, A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network, Proceedings of the 2005 International Conference on Dependable Systems and Networks, 2005.

[10] H. S. Chiu, K. S. Wong Lui, Del PHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, 1st International Symposium on Wireless Pervasive Computing, 2006.

[11] Jakob Eriksson, Srikanth V. Krishnamurthy and Michalis Faloutsos, TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks, 14th IEEE International Conference on Network Protocols, (2006), 75-84.

[12] P. Van Tran, L. X. Hung, Y. K. Lee, S. Lee and H. Lee, TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks, 2007 4th Annu. IEEE Consum. Commun. Netw. Conf. CCNC (2007), 593-598.

[13] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks, IEEE Transactionson Wireless Communications 8(2) (2009), 736-744.

[14] Shalini Jain and Satbir Jain, Detection and prevention of wormhole attack in mobile adhoc

networks, International Journal of Computer Theory and Engineering 2(1) (2010), 1793-8201.

[15] Saurabh Gupta, Subrat Kar, S. Dharmaraja, WHOP:Wormhole Attack Detection Protocol using Hound Packets, IEEE, 978-1-4577-0314-0/11,2011.

[16] Juhi Biswas, Ajay Gupta and Dayashankar Singh, WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol, 9th International Conference on Industrial and Information Systems (ICIIS), IEEE,2014.

[17] Dhruvi Sharma, Vimal Kumar and Rakesh Kumar, Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET , Computational Intelligence in Data Mining 2. Volume 411 of the series Advances in Intelligent Systems and Computing pp 475-485., Springer, 10 December 2015.

[18] Chitra Gupta and Priya Pathak, Movement Based or Neighbor Based Technique For Preventing Wormhole Attack in MANET, Symposium on Colossal Data Analysis and Networking (CDAN), 2016.

[19] Elham Zamani and Mohammadreza Soltanaghaei, The Improved Overhearing Backup AODV Protocol in MANET, Journal of Computer Networks and Communications Volume, Article ID 6463157, 8 pages. Hindawi, 2016.

[20] H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra, Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET, Tenth International Conference on Sensing Technology,(2016).

[21] Supriya Khobragade and Puja Padiya, Detection and prevention of Wormhole Attack Based on Delay Per Hop Technique for Wireless Mobile Ad-hoc Network, IEEE, 2017.

[22] Roshani Verma, Roopesh Sharma and Upendra Singh, New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA, 2017.

[23] Mohammad Rmayti and Lyes Khoukhi, Graphbased wormhole attack detection in mobile ad hoc network, IEEE, Fourth International Conference on Mobile and Secure Services (MobiSecServ), 2018.

[24] Sayan Majumdar and Debika Bhattacharyya, Mitigating Wormhole Attack in MANET using Absolute Deviation Statistical Approach, IEEE 8th Annual Computing and Communication Workshop and Conference, 317320, 2018.