Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Variants of Wormhole Attack in MANET and their Counter Measurements

Gurmeet Kaur
M.Tech (CST) Research Scholar
Central University of Punjab, Bathinda, India

Abstract*— Mobile ad hoc network is a network that is organized by itself, adaptive in nature and on an ad hoc basis. As a results of decentralized infrastructure several security problems are arise and malicious activity performed by offender. MANET routing disrupts if participating node do not perform its intended function and start performing malicious activity. A specific attack called wormhole attack basically include two malicious nodes and it enables an attacker node to record packets at one location in the network, tunnels them to another location and retransmits them into the network. In this paper, various types of MANET routing protocols, variants of wormhole attack and also the countermeasures on wormholes along with future trends have been discussed in detail.

***Keywords*— MANETs, mobility, network security, routing, tunnel, wormhole attack.**

I. INTRODUCTION

By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes having both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Due to their natural mobility and scalability, wireless networks are always preferred. The improved technology and reduced costs made wireless networks much more preferable over wired networks in the past few decades [2].

Wireless Networks can be classified into two major categories [11]:

A. Fixed Infrastructure Wireless Network

It provides communication among wireless nodes through the Access Point (AP) means nodes cannot communicate directly. The access points also work as a bridge.

B. Infrastructure less Wireless Network

It does not have any fix infrastructure for the communication. Each node can communicate directly with other node and there is no any need of the access point. An important thing is that these networks do not have routers so the wireless nodes work as routers. These networks don't have any fixed or static topology.

A mobile ad hoc network consists of mobile nodes that use wireless transmission for communication. In these types of networks the nodes can move from one place to another. The motion of the mobile nodes may be random or periodical. Thus, these networks have no fixed infrastructure, no fixed configuration and other controlling device such as router etc. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology and also they have a very less setup time. The routers are free to move randomly [11].

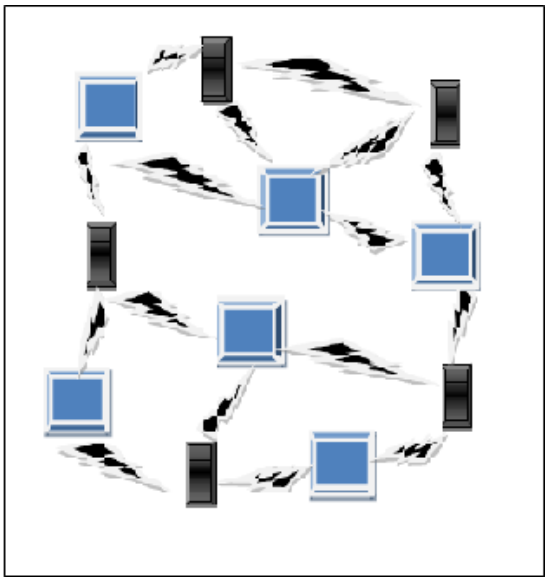

Fig. 1 Mobile ad hoc network [11]

Mobile Ad hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. Such a network is helpful in creating communication between nodes that may not be in line-of-sight and outside wireless transmission range of each other. Similar wireless networks have important applications in a wide range of areas covering from health, environmental control to military systems. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium [17]. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. The original idea of MANET started out in the early 1970s [14].

A MANET is much more vulnerable to attacks as compared to a wired network due to the following factors [3]:

- Nodes have limited energy due to which complex security solutions cannot be used.
- Transmission of routing and data packets is done in wireless medium, which is shared and generally unreliable and makes eavesdropping more likely. Even if the channel is reliable, the communication may still be unreliable due to the broadcast nature of MANETs.
- There is no central management point, which makes it difficult to ensure that all nodes participating in the network are benign.
- Mobility of nodes plays a very important role in the network, which makes routing even more challenging as the topology keeps changing regularly.

In this paper, Section II provides the MANET routing protocols. Section III refers to the wormhole and its variants, Section IV deals with the various solutions and counter measurements and Sections V highlights the conclusion and future aspects in MANET.

II. MANET ROUTING PROTOCOLS

Routing is the act of moving information from a source to a destination in a network. During this process, at least one intermediate node within the network is encountered. The routing concept basically involves two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through a network.

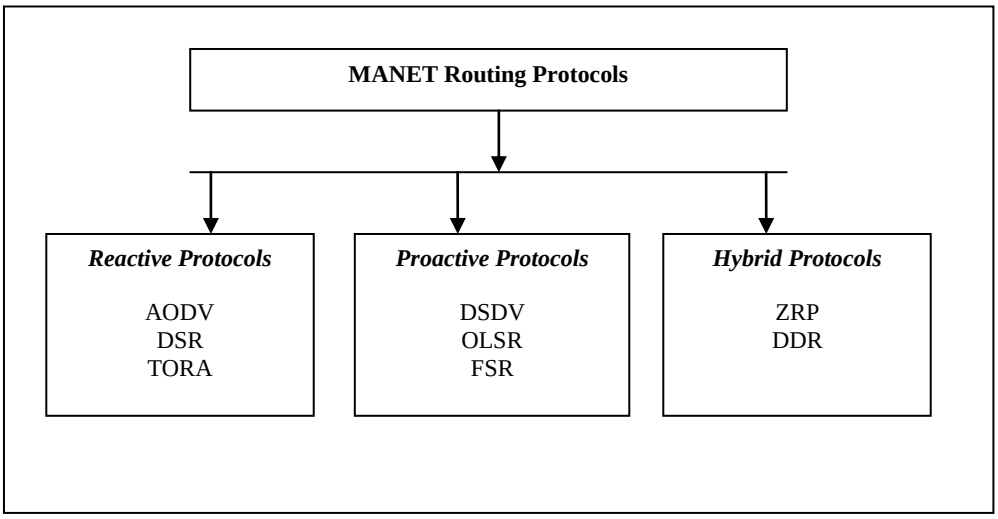

Fig. 2 MANET routing protocols [15]

The routing protocols in mobile ad hoc network can be divided into three categories [15]:

A. On-Demand (Reactive) Protocols

On demand routing protocols compute the route to a specific destination only on an on-demand basis, so a routing table containing all the nodes as entries does not have to be maintained in each node. When a source wants to send packet to a specific destination, it invokes a route discovery mechanism to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. Examples are AODV, DSR etc.

B. Table Driven (Proactive) Protocols

Proactive or table-driven routing protocols maintain the routing information consistently up-to-date from each node to every other node in the network. The main function of proactive routing protocol maintains its table in order to store routing information. Upon changing in the network topology caused by anything just need to be reflected to this table and propagate the updating information throughout the network. Examples are DSDV, OLSR etc.

C. Hybrid Protocols

These types of protocols combine the important features of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Examples are ZRP etc.

AODV is a reactive or on-demand routing protocol, which is very simple, efficient and effective routing protocol for mobile ad hoc networks which do not have fixed topology. AODV is an improvement on DSDV (Destination -

Sequenced Distance - Vector Routing Protocol) because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes in the DSDV. It uses traditional routing tables, one entry per destination. This is in contrast to DSR (Dynamic Source Routing), which can maintain multiple route cache entries for each destination [9].

III. WORMHOLE AND ITS VARIANTS

Most previous ad hoc networks research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require more secure communication and routing such as military or police networks, emergency response operations like a flood, tornado, hurricane or earthquake. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment, and the environment where they may be deployed, make them vulnerable to a wide range of security attacks [16].

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad hoc networks. During 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 that is in-band and out-of-band channel. This makes the tunnelled 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 [16].

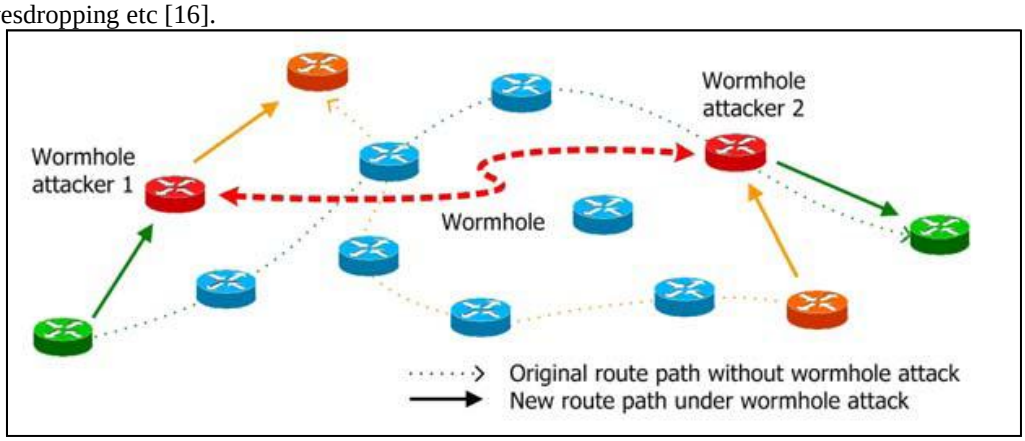

Fig. 3 The wormhole attack in MANET [18]

Wormhole attacks can be classified using different criteria as following [21]:

A. Classification based upon Implementation

This is the major classification; based upon implementation. This classification relies upon the ways the attack is launched. Wormhole attacks can be classified into the following types:

1) Using Encapsulation: In this mode, there are several nodes are involved along the path (nodes along the path may or may not be aware of wormhole) between Xs and Xd. The packet is encapsulated at Xs and travels the path in encapsulated form hence avoiding the increase in hop count. The attackers in this scenario are not connected directly to one another but make the other nodes feel that they are directly connected. The packets are transmitted using a virtual tunnel between Xs and Xd. Once successfully launched, all paths will contain a link that will comprise of link between Xs and Xd.

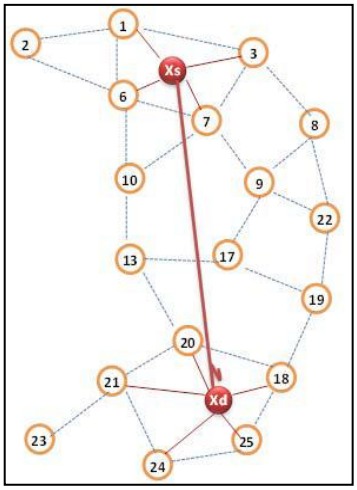

Fig. 4 Wormhole using encapsulation [21]

2) Using Out-Of-Band Channel: The colluder nodes are directly connected through a high bandwidth out of band channel. The channel can be achieved by a wired connection or using a wireless channel which is long range and directional. Due to the requirement of extra hardware it is difficult to launch, but provides an ease because it will not need any encapsulation/decapsulation since the colluders are directly connected.

3) Using High Power Transmission: This particular type of wormhole is launched from two colluder nodes that have a high power transmission capability.

4) Via Protocol Deviations: The attackers in such case create the wormhole by not following the protocol rules, for an example, some of the protocols assume the nodes to wait for some time before retransmitting. But the attackers do not comply with this rule and keeps on broadcasting without back off and thus trying to arrive first at the destination and thereby avoiding any future legitimate requests to reach destination. Even if the future requests reach destination, they will be dropped, since a request passing through the colluder has already been received.

B. Classification based upon Medium Used

Wormhole attacks can also be classified as In-Band and Out-Of-Band wormhole attacks.

1) In-Band Wormhole: Attackers are using the same medium for creating link between them, for example encapsulation, packet relay and protocol deviations.

2) Out-Of-Band Wormhole: Attackers are not using the same medium as normal network nodes, for example out-of-band channel and high transmission mode.

Wormhole can be formed using in-band channel where malicious node W1 tunnels the received route request packet to another malicious node W2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following W2 nodes believe that there is no node between W1 and W2. Second, out-of-band channel where two malicious nodes W1 and W2 employ a physical channel between them by either dedicated wired link or long range wireless link shown in Fig. 5 [16]. When malicious nodes form a wormhole or tunnel, then they can reveal themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the latter is a hidden or close one. In Fig. 5, the destination D notice that a packet from the source S is transferred through node A1 and B1 under hidden wormhole attack, while it believes that the packet is delivered via node A1, W1, W2, and B1 under exposed wormhole attack [16].

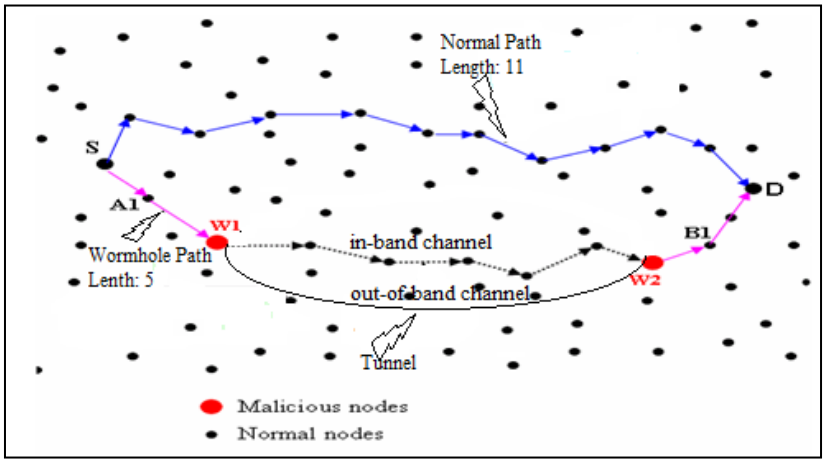

Fig. 5 Wormhole Attack [13]

C. Classification Based upon Attackers

1) Self-Sufficient: Where colluders advertise themselves as normal nodes, all paths passes through them, for example out-of-band channel or using high power transmission.

2) Extended Wormhole: The colluders are hidden by themselves and extend the attacks beyond themselves to normal nodes, for example encapsulation or packet relay.

D. Classification Based upon Location of Victim Nodes

1) Simplex: Victim node lies in range of only one attacker.

2) Duplex: Victim node lies in range of both the attackers.

So, in any ad hoc network, a wormhole can be created through the following three ways [13]:

- Tunnelling of above the network layer.
- Tunnel creation via internal hidden infrastructure (hidden wormhole attack).
- Tunnel creation via external wired infrastructure (exposed wormhole attack).

Sometimes, to identify the nodes involved in wormhole attack, some of the parameters used are strength, length, attraction and robustness as follows [12]:

- *Strength:* It measures the amount of traffic forwarded by the tunnel which is advertised by the two colluding nodes.

- *Length:* Length is measured by the difference in number of hops between the genuine shortest path and the advertised path by malicious nodes.
- *Attraction:* Attraction means the reduction in the path length offered by the wormhole. When the attraction has low value, then the small improvement in the actual path may reduce its strength.
- *Robustness:* Robustness refers to the persistence of nodes creating wormhole even a small change in the topology of the network.
- *Packet delivery ratio:* It is the ratio between number of delivered packets and total number of dispatched packets.

IV. COUNTER MEASUREMENTS

Wireless networks are playing very important role in the present world. Mobile Ad hoc Networks (MANETs) are the extension of the wireless networks. These networks are playing crucial role in the each and every field of the human life. They are used in those places where a simple wireless network cannot use. Due to their adaptive nature they are threatened by number of attacks. Wormhole attack is one of the dangerous active attacks in the mobile ad hoc networks [6]. Various solutions and countermeasures have been proposed to detect and prevent wormhole attack.

A. Packet Leashes

Packet Leashes method is used to defend against the wormhole attack. It uses the TIK protocol based on TESLA and also uses temporal leashes to determine the wormhole attack by transmission time. Two types of leash information were used Geographical Leash and Temporal Leash. In geographical leashes each node must have its accurate location information and loose clock synchronization. When node receives a packet, it calculates distance between previous node and itself by using send/receive time stamp. For temporal leashes, each node should have accurate clock synchronization. Every packet should be delivered to the next node within computed life time of a packet. Otherwise, the next node regards the path as a wormhole [20].

B. DELPHI

It is a delay analysis approach called DELPHI (Delay Per Hop Indicator). It calculates mean delay per hop of every possible route. DELPHI applied a multi-path approach and recorded the delay and hop counts in transmitting RREQ and RREP through the paths. After collecting all response, the sender computes mean delay per hop of each route. The path with wormhole attacks, the delay would be obviously longer than a normal path with the same hop count. Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided and DELPHI protocol does not identify the malicious nodes which were making wormhole in the network [4].

C. LITEWORP

LITEWORP use the notion of guard node. The guard node can detect the wormhole if one of its neighbors is behaving maliciously. The guard node is a common neighbor of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link [5].

D. WARP

A modified AODV routing protocol called WARP to defend against wormhole nodes by adopting link disjoint multi-path routing between source and destination. In WARP each node records all of its neighbor's anomaly values (number of times it forms path from different source to destination). Due to wormhole node's great ability to grab routing paths, if the occurrence of one links exceeds the threshold value, the two ends of this link may be wormhole nodes. If anomaly values of a node exceed a threshold value then its neighbor will discard all requests for forming route containing that node in the path [8].

E. WHOP

An approach named WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and designed to detect wormhole attack with the help of hound packets. In this approach a hound packet is sent after the route discovery process, means after the route has been discovered. This hound packet is processed by all the nodes, except that nodes which are involve in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and signed this message digest with its own private key and attached all this information with the hound packet. But processing delay of the packet becomes high [16].

F. MHA

A new protocol called Multi-path Hop-count Analysis (MHA), using hop-count analysis without any special environment assumptions to avoid wormhole attack. Hence, it can be directly used in MANET. It is assumed that too low or too high hop-count is not healthy for the network. Furthermore, MHA is designed to use split multi path routes, so the transmitted data is naturally split into separate route. An attacker on a particular route cannot completely intercept (and subvert) the content. The proposed scheme has high efficiency and very good performance with low overhead [18].

G. PTT

It is a Packet Travel Time Algorithm for detecting wormhole attacks, whether in hidden or exposed mode in wireless multi-hop net-works without special hardware. This algorithm is an improvement on another algorithm which is based on transmission time-based mechanism (TTM). Moreover, our algorithm introduces a new mechanism called Packet Travel Time (PTT). This mechanism allows each device to monitor its neighbors' behavior. Therefore, this mechanism can detect both hidden and exposed wormhole attacks, and can locate the wormhole in AODV and DSR protocol [1].

H. Topological Comparison Based Method

A new detection mechanism called RTT-TC, which is based on round trip time measurements and topological comparisons, was also introduced for the detection of wormhole attack. The scheme is based on the following two

observations of wormhole attacks: Two fake neighbors with a wormhole tunnel in between has longer RTT, compared to the RTT with true neighbors and Two true neighbors usually share other true neighbors between them, and two fake neighbors do not share common true neighbors. The first rely is on RTT measurements to identify suspected wormhole attacks and then use of topological comparison to exclude genuine neighbors from the suspected list [7].

I. Using Routes Redundancy and Time-based Hop Calculation

It is a method to detect and isolate wormhole attacks in mobile ad hoc networks (MANETs). It is used to create many possible routes when sending Route Request (RREQ) from source to destination and to use those routes as reference of each other, in order to find malicious nodes with suspicious behavior within the network. The proposed method works in three steps, which are using routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes. Routes redundancy is started where source sends RREQ using every possible way to destination. All routes that connect source and destination are listed together with the number of hops from every route. Some routes gathered in the same relay point before destination is aggregated, so all nodes that join the network can be listed and the behavior of malicious nodes in can be detected. The RTT and number of hops of all listed routes are compared in order to detect suspicious route. Nodes with suspicious behavior within network are isolated and will not be considered for transmission. This scheme does not require additional hardware such as GPS devices and it ensures that request received by destination. Simulation results show that the proposed scheme is able to isolate the wormhole attacks and able to hold the increasing of packet dropped compare to AODV approach and time-based calculation [19].

J. Using Detection Packets

A general mechanism, without use of hardware, location information and clock synchronization called detection packet (modification of hound packet) for detecting and preventing wormhole nodes in network, which is based on DSR routing protocol. Detection packet has three fields: Processing Bit, Count to Reach Next Hop and Time Stamp (TS). Timestamp is used for strongly detection with conformance at wormhole attack. Finally, improve throughput, packet delivery ratio (PDR) and reduce end to end delay [13].

K. *Hybridized WHOP*

A reactive routing approach for preventing wormhole attack to reduce the process delay time, using the idea of hybridize WHOP protocol with time synchronization mechanism. The proposed approach provides efficient results to secure data packet transmission and reduces the process delay time while not use of any expensive hardware by using DSR protocol [10].

TABLE I
WORMHOLE ATTACK DETECTION PROTOCOLS [4], [5], [8], [16], [20]

Protocol	Based on	Extra Hardware	Clock Synchronization	Work for Out-Of-Band Wormhole	Work for In-Band Wormhole	Identify Wormhole Nodes
TIK	None	Yes	Yes	No	Yes	Yes
DELPHI	AODV	No	No	Yes	Yes	No
LITEWORP	DSR	Yes	Yes	Yes	Yes	Yes
WARP	AODV	No	No	Yes	Yes	Yes
WHOP	AODV	No	No	Yes	Yes	Yes

TABLE II
WORMHOLE ATTACK PREVENTION MECHANISMS [10], [13]

Mechanism	Based on	Extra Hardware	Clock Synchronization	Prevent Wormhole Nodes	Performance Parameters
Detection Packets	DSR	No	No	Yes	PDR, Throughput, Delay
Hybridized WHOP	DSR	No	Yes	Yes	PDR, Throughput, End to End Delay

V. CONCLUSION AND FUTURE WORK

In this paper, MANET routing protocols, various classifications of wormhole attack and their different countermeasures have been discussed. A wormhole attack is a very serious threat to the important security objectives (Confidentiality, Integrity and Availability) of the mobile ad hoc network and it must be treated as a highest priority threat. As we know that mobility of nodes plays a very important role in the network, which makes routing even more challenging as the topology keeps changing regularly. In our future work, we will be emphasizing more on the wormhole attack–defense mechanism. Till now, many approaches have been developed for the detection and isolation of these

wormhole nodes but these mechanisms do not take into account the impact of different mobility models. Our research would be focused on proposing and developing a defense mechanism with impact of mobility models for the detection of wormhole attack.

REFERENCES

[1] A.S. Alshamrani, "PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks", *2011 Workshops of International Conference on Advanced Information Networking and Applications*, pp. 561-568, 2011.

[2] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK – A Secure Intrusion – Detection System for MANETs", *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089-1098, March 2013.

[3] H. Ehsan, and F. A. Khan, "Malicious AODV", *11th International Conference on Trust, Security and Privacy in Computing and Communication, IEEE Computer Society*, pp. 1181-1187, 2012.

[4] H.S. Chiu, and K.S. Lui, "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", *1st International Symposium on Wireless Pervasive Computing*, pp. 6–11, Jan. 2006.

[5] I. Khalil, S. Bagchi, and N.B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *International Conference on Dependable Systems and Networks*, pp. 612–621, 2005.

[6] K. K. Joshi, N. Khemariya, and D. Chaudhary, "An Efficient Algorithm based on Fibonacci Pattern Hound Packets for Detection of Wormhole Attack in DSR for Mobile Ad Hoc Networks", *International Journal of Computer Applications*, vol. 63, no. 11, pp. 23-28, Feb. 2013.

[7] M. R. Alam, and K. S. Chan, "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", *IEEE Transactions*, pp. 991-994, 2010.

[8] M. Y. Su, "WARP: A Wormhole Avoidance Routing Protocol by Anomaly Detection in Mobile Ad Hoc Networks", *Computers & Security*, vol. 29, pp. 208-224, March 2010.

[9] N. I. Sarkar, and W. G. Lol, "A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility", *IEEE Personal Communications*, pp. 515-520, 2010.

[10] N. Jain, and A. K. Shrivastava, "Reactive Routing Approach for Preventing Wormhole Attack using Hybridized WHOP", IOSR Journal of Computer Engineering, vol. 13, pp. 87-95, Aug. 2013.

[11] N. Khemariya, and A. Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", *International Journal of Computer Applications*, vol. 66, pp. 18-24, March 2013.

[12] N. Satheesh, and Dr. K. Prasadh, "Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 708-713, Sept. 2013.

[13] P. Nayak, A. Sahay, and Y. Pandey, "Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet", *International Journal of Scientific & Engineering Research*, vol. 4, pp. 1216-1222, June 2013.

[14] R. Maulik, and N. Chaki, "A Study on Wormhole Attacks in MANET", *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 3, pp. 271-279, 2011.

[15] S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Scenario – based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET", *2012 International Conference on Computer Communication and Informatics*, 2012.

[16] S. Gupta, S. Kar, and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", *International Conference on Innovations in Information Technology, IEEE Transactions*, pp. 226-231, 2011.

[17] S. Mehta, and Dr. M. Sharma, "Analysis of Black Hole and Wormhole Attack using AODV Protocol", *International Journal of Research in Management, Science & Technology*, vol. 1, pp. 44-48, June 2013.

[18] S. M. Jen, C. S. Laih, and W. C. Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", *Sensors*, pp. 5022-5039, June 2009.

[19] S. Y. Shin, and E. H. Halim, "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation", *IEEE Transactions*, pp. 781-786, 2012.

[20] Y.C. Hu, A. Perrig, and D. B. Johnson, "PACKET LEASHES: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", *IEEE INFOCOM*, pp. 1976–1986, 2003.

[21] Z. A. Khan, and M. H. Islam, "Wormhole Attack: A New Detection Technique", *IEEE Transactions*, 2012.

