A Comprehensive Study on Defence Against Wormhole Attack Methods in Mobile Ad hoc Networks

Reza Fotohi , Shahram Jamali
Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
Fotohi.reza@gmail.com
Department of Computer Engineering, University of Mohaghegh ardabili, Ardabil, Iran
Jamali@iust.ac.ir

Abstract

A mobile ad hoc network (MANET) contains a collection of wireless mobile nodes that forms a temporary network without having any fixed infrastructure or centralized administration. MANET is assailable to routing misbehaviour. We are worried of an especially severe security attack that affects the MANET routing protocols, it is called the wormhole attack. During the attack an attacker captures packets from one location in the network, and tunnels them to other attacker at a distant point, which replays them locally. In this paper, we examine briefly the behavior of various Denial-of-Service attacks at the network layer of MANET and provide comprehensive survey of on wormhole attack and introduce the existing defense approaches to these attacks.

Keywords*:* MANETs, Wormhole attack, AODV, DSR.

I. INTRODUCTION

With the rapid development in wireless technology, ad hoc networks have emerged in several forms. These networks act in the license free frequency band and don't require any investment in infrastructure, making them attractive for military and selected commercial applications. However, there are lots of unsolved problems in ad hoc networks; securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons; amongst them are lacks of secure boundaries, threats from compromised nodes within the network, lack of centralized management facility, restricted power supply, scalability (Yudhvir et al, 2013).

One of the hazardous security attacks is a wormhole attack, which has been introduced in the context of ad hoc networks. In this attack, a attacker captures packets from one point in the network, and tunnels them to another attacker at a distant point, which replays them locally. The tunnel can bee established in many different ways, e.g., through an out-of-band hidden channel, a packet encapsulation, or a high powered transmission. This makes the tunneled packet come either sooner or with a lesser number of hops compared to the packets transmitted over ordinary multi hop routes. This builds the imagination that the two end points of the tunnel are very close to each other (Capkun et al, 2003)(Wang et al, 2006)(Hu et al, 2006)

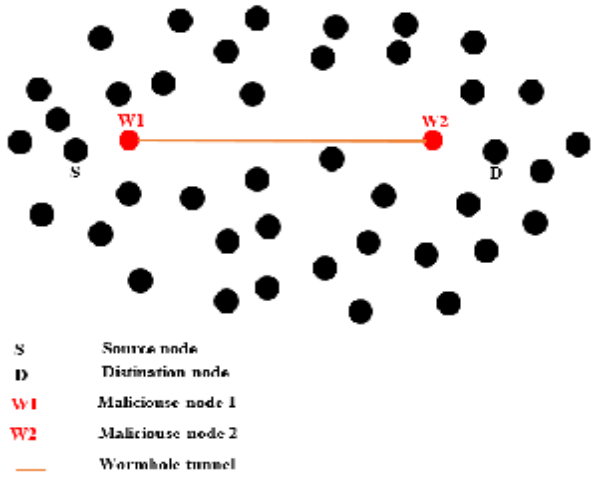


Figure.1. Mobile ad hoc network with wormhole attack ; (Karthik et al, 2012)

.

Fig.1 shows an example of wormhole attack. A network under a wormhole attack. Attackers w1 and w2 are connected by an out-of-band channel link, which they use to tunnel network data from one end of the network to the other.

This paper survey of the existing defense approaches to these attack.

A. Paper Organization

Section 2 of this paper presents the routing protocol in MANET. In Section 3, we present the security issues. Section 4 presents network layer attacks. In Section 5, we present the wormhole attack and related work. and Section 6 presents the conclusion.

II. ROUTING PROTOCOLS IN MANET

In this section we give a brief overview on the Ad Hoc on Demand Distance Vector (AODV) routing protocol in MANET.

A. Overview of Ad Hoc on Demand Distance Vector (AODV)

(Perkins et al, 2004) AODV is a routing protocol for MANETs and other wireless ad-hoc networks. It is jointly extended in nokia research centre of university of california, santa barbara and university of cincinnati by C. Perkins and S. Das. It is an on demand and distance vector routing protocol, concept that a route is build by AODV from a destination only on demand. AODV is able to each two unicast and multicast routing. That maintains these routes since they are desirable by the sources. Furthermore, AODV builds trees which connect multicast group members. The trees are combined of the group members and the nodes needed to join the members. The sequence numbers are used through AODV to guarantee the being fresh of routes. It is loop-free, self-starting, and scalable to great numbers of mobile nodes.

1) Messages in AODV

There are four control messages are used by AODV explained as follows.

Routing Request (RREQ): Since a route is not available for the destination, a RREQ packet is flooded throughout the network which includes the below format.

Src Add	Request ID	Source Seq No	Dest Add	Dest Seq No	Hop Count

Figure.2. RREQ Format

Routing Reply (RREP): If a node is the destination, or has a valid route to the destination, it unicast RREP message back to the source, which has below format.

Src Add	Dest Add	Dest Seq No	Hop Count	Life Time

Figure.3. RREP Format

Route Error Message (RERR): All nodes monitor their own neighborhood and broadcast message when: A node detects that a link with adjacent neighbor is broken.

Unreachable Dest IP Add	Unreachable Dest Seq No

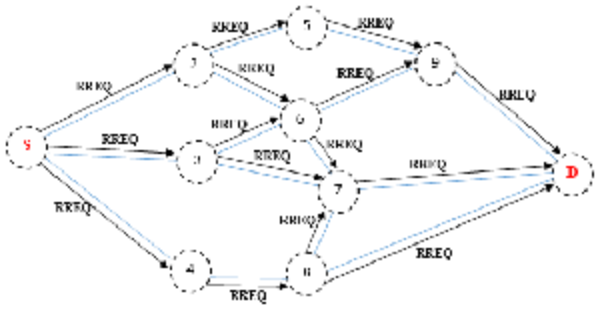
Figure.4. RERR Format

HELLO Messages: Each node can get to know its neighborhoods by using local broadcasts, so called HELLO messages.

2) Working of AODV

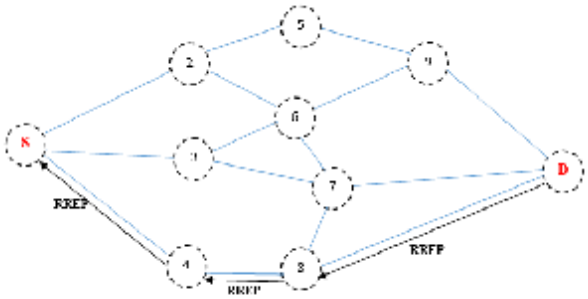
a) Route Discovery

In on demand routing protocol AODV (Fotohi et al, 2013), when a source node wants to communicate with a destination node for data packet delivery, source node initiates route discovery process by broadcasting RREQ packet. Until destination node is discovered, every intermediate node floods RREQ by rebroadcasting. AODV limits this flooding by considering first received RREQ. When destination node or an intermediate node having valid route to destination, receives RREQ, it sends back RREP towards source. Source receives RREPs from different path and selects RREP of shortest hop-count for selecting data delivery path.



(a) Propagation of RREQ Packet

May.2014-Volume 2.No5
ISSN 2345-3397



(b) Patch taken by the RREP Packet

Figure.5. Route discovery in AODV

b) Route Maintenance Stage

A hello message is broadcasted by active nodes periodically. If no hello message from a neighbor, then upstream node will notify the source with an RERR packet and entire routes based on the node is cancel. Source will initialize a new route discovery step and flood the RREQ packet (Benjamin et al, 2004) (Fotohi et al, 2013). The above procedure can be realized in the below figure.

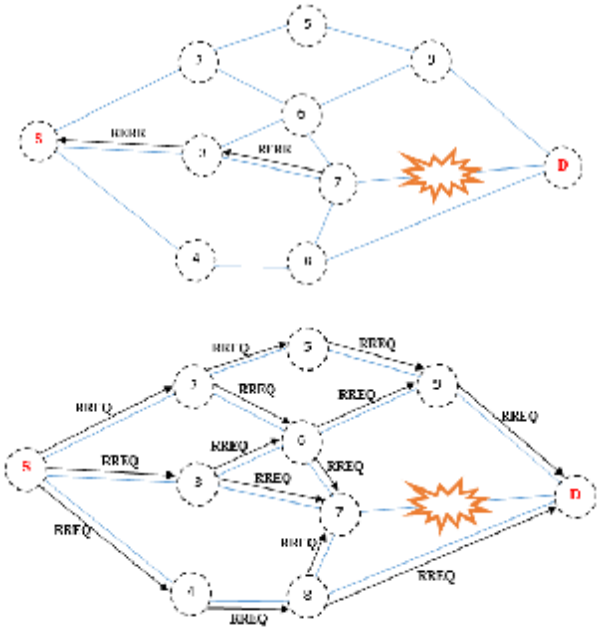
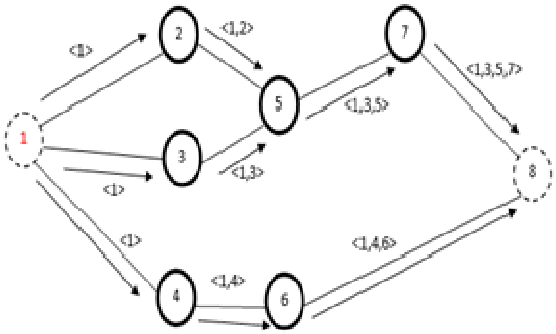


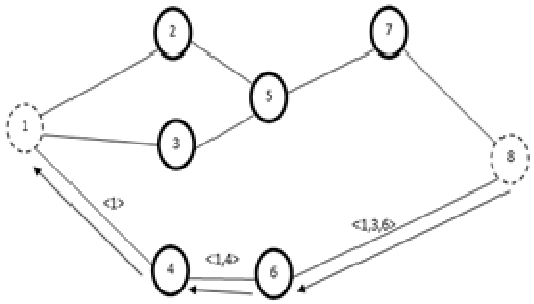
Figure.6. Route maintenance in AODV

B. Dynamic source routing (DSR)

DSR protocol is an on demand routing protocol based on the concept of source routing, which means that the initiator knows the complete hop-by-hop route to the destination. This specific feature brings performance, but also results in the scaling of routing message overhead. To perform DSR, each node is required to maintain a route cache which contains the topology information of the network. The route cache is consistently updated to reflect the current status of the network. DSR consists of two major phases: route discovery and route maintenance. In case of route recovery, source node generates RREQ and broadcasts its to neighbors. The receiving node will append its own address to the RREQ packet and rebroadcasts it, if it is not the destination. On reception of RREQ packet at destination, node generates RREP packet and forward back to the source, as shown in Fig. 7 (Qazi et al, 2013).



(a) Propagation of RREQ Packet



(b) Patch taken by the RREP Packet

Figure.7. Route discovery in DSR

III. SECURITY ISSUES

Due to lack of reliable centralized administration, limited bandwidth, limited power, wireless links, dynamic topology and easy eavesdropping MANETs are more sensitive to security attacks than existing conventional networks (Hoang et al, 2006). A network should achieve aims such as availability, integrity, confidentiality, authentication and non repudiation (Rutvij et al, 2012), that are described in the below (Korbakorba et al, 2013):

- **Availability:** Generally aims denial of service (DoS) attacks and is the ability to sustain the networking functionalities without any interruption because of security threats.
- **Integrity:** ensures that a packet is not modified during transmission.
- **Confidentiality:** ensures certain information is never disclosed to unauthorized entities.
- **Authentication:** ensures that the other end of a connection or the originator of a packet is the node that is claimed.
- **Non Repudiation:** ensures that the origin of a message cannot deny having sent the message.

Due to inherent specifications of MANETs, they face many security issues compared to present ordinary networks (Hoang et al, 2006). An attacker can contravention them by passively or actively attacking on MANETs (Rutvij et al, 2010). A passive attack is difficult to detect as the adversary obtains information without disturbing normal network operations; traffic analysis, traffic monitoring and eavesdropping are examples of passive attacks. On the other hand, active attack can be internal or external in which adversary alters information and thus, disturbs network operations; examples of such attack are impersonation, modification, fabrication, jamming, message replay, denial-of service. TABLE I. shows the characteristics and examples of active and passive attacks. Both active and passive attacks can be launched on any layer of the network protocol stack. Table II. The paper (Perkins et al, 2004) shows some examples of attacks on different layers.

We carried out study of some network layer attacks as discussed in (Rutvij et al, 2012) and. (Rutvij et al, 2012). In this paper, we further study wormhole attack and investigate existing defense mechanisms in the V section.

TABLE I
PASSIVE AND ACTIVE ATTACKS

Type of Attack	Characteristics	Examples
Passive Attacks	Obtains information without disturbing normal network operation Difficult to detect	Traffic analysis, traffic monitoring and eavesdropping
Active Attacks	Can be internal (attacker within the network) or external (attacker outside the network) Can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node	Modification, impersonation, fabrication, jamming and message replay

TABLE II
ATTACKS ON DIFFERENT LAYERS OF PROTOCOL STACK

Layer	Examples of Attacks
Application Layer	o Repudiation, Data corruption, Viruses, Worms, Malicious codes
Transport Layer	o Session hijacking, SYN flooding
Network Layer	o Sybil attack, Sinkhole attack, Blackhole attack, Grayhole attack, Wormhole attack, Spoofing, Flooding, Location disclosure, Route table overflow, Route table poisoning, Route cache poisoning
Data-link Layer	o Traffic monitoring and analysis, Disrruption MAC (802.11), WEP weakness
Physical Layer	o Jamming, Interception, Eavesdropping

IV. NETWORK LAYER ATTACKS

Attackers trying to modify messages or generate false messages take down the network's operations which causes denial of service in MANETs. In this section we summary introduce various attacks, discuss their proposed countermeasures and try to find their restrictions (Rutvij et al, 2012).

A. Sybil attack

In sybil attack, a attacker presents multiple addresses and behaves as if it were a group of nodes. There are, mainly, two different ways through which a sybil node can get an identity; stealing other node's identity or fabricating fake identities. By impersonating a large number of nodes in the network, the attacker forbids other nodes from using those addresses; it can escape from detection systems. This attack can strongly harm geographic routing protocols, and can even threat multiple path routing schemes and node localization (Hu et al, 2003).

B. Sinkhole attack

A sinkhole attacker places itself at very strong status in the network and informs a high quality route to destination or spoofs neighboring nodes that are neighboring the destination. The compromised node at the sinkhole's heart could then perform selective forwarding, packet dropping or data manipulation (Roy et al, 2008).

C. *Blackhole attack*

Blackhole attack is another type of DoS attack that generates and disseminates build routing information. As mentioned in (Mohammad et al, 2004), a attacker, exploiting the flooding based routing protocol, advertises itself as having a valid shortest route to the destined node. If the attacker replies to the requesting node before the actual node replies, a bogus route will be created. Hence packets are not forwarded to the certain destination node; instead, the attacker intercepts the packets, drops them and thus, attracts network traffic (Anu et al, 2009).

D. *Grayhole attack*

We now explain the gray hole attack on MANETs. The gray hole attack has two stages. In the first stage, a attacker exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second stage, the node drops the intercepted packets with a certain probability. This attack is harder to detect than the black hole attack where the attacker drops the received data packets with certainly. A gray hole may display its attacker behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also display a behavior which is a combination of the above two, thereby making its detection even more difficult (Pradip et al, 2010)

.

E. *Selfing attack*

The successful work of MANET is completely relevent on the collaboration of participating nodes in communication. Selfing attacks which participates in the routing protocol correctly but does not forward the data packets to the destination node. The attacker may drop all or few of the packets that are routed via that node to preserve its resources or to satisfy any other motives (Ehsan et al, 2012).

F. *Flooding attack*

In MANET, a DoS attack can be easily setup by flooding numerous request packets or data packets; a attacker may send request packets in a short time to the destination node which does not exist in the network; as no one sends reply, whole network will be flooded with the request packet, such as case occurs with data packet flooding where a misbehaving source node continuously sends useless data packets to destination exhausting system resources. Because of limited resource capacities of a mobile node such as limited battery power, limited memory space, limited computational ability and limited bandwidth capacity, it cannot provide services when it receives a flood of packets. Therefore, the victim node or sometimes the whole network can get easily paralyzed (Hyojin et al, 2010).

G. *Wormhole attack*

Also called tunneling attack, it is one of the most sophisticated attacks in MANETs. In this attack, a attacker captures data packets from one point in a network and tunnels them through an out of band channel to another attacker located several hops away, which relays them to its neighboring nodes. The tunnel between the attackers is actually faster than links between legitimate nodes, so the tunneled packets arrive sooner than packets through other routes. Therefore, the attackers are more likely to be included in the route and take an advantage for future attack. Detection of wormhole attack is generally difficult, and requires the use of an unalterable and independent physical metric, such as time delay or geographical location (Kim et al, 2008).

V. TAXONOMY OF WORMHOLE ATTACK AND RELATED WORKS

A. *Taxonomy of wormhole attack*

In preview works (Mahajan et al, 2008), (Chiu et al, 2006), (Maulik et al, 2010); wormhole attacks are classified using different criteria. Wormhole attacks can be classified based upon:

1) Its Implementation, 2) The medium used,
3) The attackers 4) The location of victim nodes.

1) Classification based upon Implementation:

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

a) Using Encapsulation:

In this case, there are several nodes are involved along the path (nodes along the path may or may not be aware of wormhole) between w1 and w2. The packet is encapsulated at 2 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 tunnel between w1 and w2. When successfully launched, all paths will contain a link that will comprise of link between w1 and w2.

b) Using out-of-band channel:

The attackers are directly connected through a high bandwidth out of band channel. The channel can be achieved by a wireless channel which is long range and directional. Because of the requirement of extra hardware it is difficult to launch, but provides an ease because it will not need any encapsulation or decapsulation since the attackers are directly connected.

c) Using high power transmission:

This specific type of wormhole is launched from two attackers that have high power transmission ability.

d) Via protocol deviations:

The attackers in such mode build the wormhole by not following the protocol rules, e.g. 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 next requests reach destination node, they will be dropped, since a request passing through the attacker has already been received. Please note that some protocols only anticipate the first request and drops all copies of the same request that arrive in next.

2) Classification based upon Medium Used:

Wormhole attacks can be also classified as in band and out of band wormhole attacks.

a) In band wormhole:

Attackers are using the same medium for building link between them e.g. encapsulation, packet relay and protocol deviations.

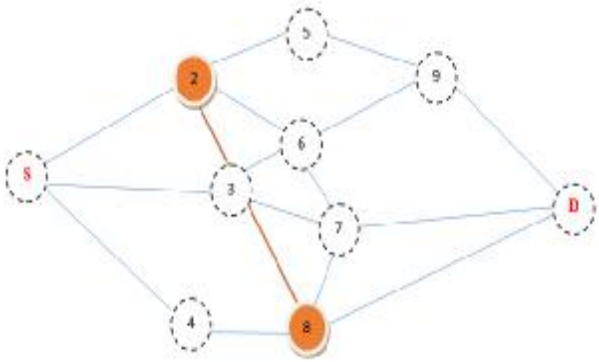


Figure.8. In band wormhole

b) Out of band wormhole:

Attackers are not using the same medium as normal network nodes, e.g. out of band channel and high transmission mode.

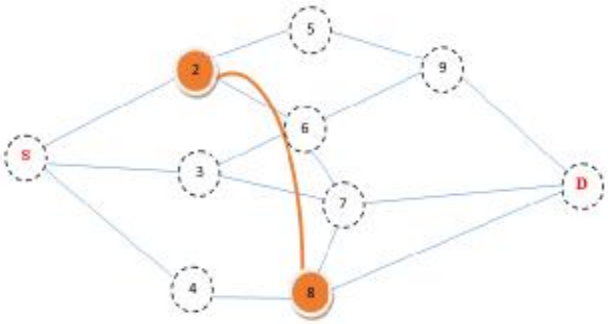


Figure.9. Out-of-band wormhole

3) Classification based upon Attackers:

a) Self Sufficient:

Where attackers advertise themselves as normal nodes, all paths passes through them e.g. out of band channel or using high power transmission.

b) Extended wormhole:

The attackers are hidden by themselves and develops the attacks beyond themselves to normal nodes e.g. encapsulation or packet relay.

4) Classification based upon location of Victim nodes

a) Simplex:

Victim node lies in range of only one attacker.

b) Duplex:

Victim node lies in range of both the attackers.

B. Related Works

The methods proposed in literature to defend against wormhole attacks can be divided into three categories.

The **first** is to modify a well known routing protocol, as AODV[1] (Perkins et al, 2004) or DSR[2] (Benjamin et al, 2004), to avoid wormhole nodes during path discovery, such as (Song et al, 2005)(Chiu et al, 2006)(Lee et al, 2008)(Su et al, 2007)(Abdesselam et al, 2008).

The second is to adopt additional hardware, such as a positioning system, a time synchronization mechanism or a directed antenna, in addition to changing the routing protocol. Some of which are (Hu et al, 2006)(Khalil et al, 2005)(Khalil et al, 2006)(Wang et al, 2007)(Marianne et al, 2008) and in (Capkun et al, 2003), two mechanisms are introduced to detect wormhole attacks: temporal packet leashes and geographical packet leashes. In temporal leashes, accurate clock synchronized clocks are used to restrict the propagation time of packets. In geographic leashes, loose clock synchronization and location information are used to restrict the migration distance of packets. Anyway the clock synchronization and location information must be obtained via additional hardware, e.g., GPS or other positioning systems (Petrova et al, 2011)(Aloudat et al, 2011)(Zhou et al, 2013). Moreover, both temporal and geographical leashes are required to add authentication information to each packet, which take up huge amounts of storage. In (Hu et al, 2004), directional antennas are used to prevent wormhole attacks. Nodes use directional antennas to transmit packets to their neighbour nodes in a particular direction. It is also assumed that all antennas on nodes are aligned. The process of neighbour discovery is implemented in a secure way using directional antennas. Anyway, it is maybe impossible to deploy directional and aligned antennas on all of mobile nodes in practice.

Finally, the third is to deploy an intrusion detection system (IDS) with or without hardware support, such as (Gorlatova et al, 2006)(Marianne et al, 2008)(Wang et al, 2006)(Phuong et al, 2007). Since the proposed approach in this paper is a secure routing protocol (e.g., DSR) without hardware support, only those researches belonging to the first category are introduced as follows.

(Lee et al, 2008) Proposed a modified DSR protocol to defend against wormhole nodes by adopting a multi path routing method. A source node start route discovery, and the destination node, after receiving multiple paths, begins to compute the proportion of every link between two nodes in the total paths. Because of wormhole node's great capability to grab routing paths, if the occurrence of one link exceeds the threshold amount, the two ends of this link may be wormhole nodes. The destination node would initials send a test data packet to verify if this link is unusual, such as the packet being dropped. If it's confirmed that the two ends of this link are wormhole nodes, the destination would send a notice message to the neighbours of the attackers, informing them not to process any messages from the attackers. In this way, the attackers would be isolated, and then quarantined. (Su et al, 2007) Proposed an AODV based routing protocol, named DelPHI, to defend against wormhole attacks. DelPHI also applied a multi path mechanism, and recorded the delay and hop counts in transmitting RREQ and RREP (actually named DREQ and DREP in DelPHI) via the paths. In this way, the average time taken by each hop can be computed. In the case of a path subjected to wormhole attacks, the delay would be obviously longer than a normal path with the same hop count (i.e., the wormhole nodes may have a heavy load, and so, packet processing is slow). Therefore, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided. In (Qian et al, 2005), a SAM[3] is proposed to detect wormhole attacks in the network adopting multi-path routing protocol. Because of tunnelling by wormhole nodes, the number of hops of the path with wormhole nodes appears to be smaller than usual paths. Thus, the routing path with the wormhole nodes is more attractive to routing discovery of the sources. Via statistics computation of relative frequency of each routing path, the path that has the largest relative frequency is identified as the path with the wormhole nodes. However, the bug is that, in non multipath routing protocol as AODV, this proposal cannot work.

[1] Ad hoc On Demand Distance Vector
[2] Dynamic Source Routing
[3] Statistical Analysis of Multipath

In (Su et al, 2009), the authors propose a secure routing protocol based on the AODV routing protocol: WARP[4]. It does not require any hardware. It considers link-disjoint multi-paths during path discovery, and supplies greater path selections to avoid attackers, but eventually uses only one path to transmit data. Based on the specifications that wormhole nodes can easily grab the route from source node to destination node, WARP enables the neighbours of the wormhole nodes to discover that the wormhole nodes have abnormal path attractions. Then, the wormhole nodes would be gradually isolated by their normal neighbouring nodes, and finally be quarantined by whole network. However, some nodes may be misjudged to be wormhole nodes because they are located at the key positions of connectivity within the network.

In (Khalil et al, 2006) proposed a scheme in which each node must broadcast messages that can be transmitted over 2 hops. Each node records the neighbouring list of one hop and two hops, as well as the corresponding session keys. When a node received a routing message without a valid MAC[5], there may be wormhole attacks. The purpose of maintaining a two hops neighbouring list by each node is to allow the node to recognize if a wormhole attack is a hidden wormhole attack or an exposed wormhole attack, as wormhole nodes may disclose themselves or hide themselves in a routing path. The former is an exposed wormhole attack, while the latter is hidden.

(Su et al, 2007) Proposed a routing protocol to alleviate wormhole attacks. This protocol is a modification of the Ariadne (Petrova et al, 2011) routing protocol, and can only defend against in-band (or packets encapsulated) channels of wormhole attacks (Mahajan et al,2008). Their method calculates the average time in transmitting RREQ through normal nodes, so that a normal node can distinguish a particularly long duration in transmitting an RREQ when malicious nodes executing in-band wormhole attacks. (Petrova et al, 2011) Used four message exchanges to defend against wormhole attacks in the OLSR[6] based routing protocol, as wormhole nodes should process a great amount of packets, causing longer delays of packets than in normal nodes. The authors mainly used HELLO and ACK messages as the messages to confirm the delay. Table III. shows brief description of various approaches for detection or prevention against a wormhole attack and their limitations.

[4] Wormhole Avoidance Routing Protocol
[5] Message Authentication Code
[6] Optimized Link State Protocol

TABLE III
WORMHOLE DETECTION/PRVENTION TECHNIQUES

Reseacher	Year	Techniques	Description	Restrictions
Capkun at al.	2003	The SECTOR protocol	allowing nodes to prove their encounters with other nodes. However, several hypotheses are needed for this protocol to work correctly. Among these are the necessity for coarse synchronization, the ability of nodes to measure their local timing with nanosecond precision, the pre-establishment of security associations between each pair of nodes, and the presence of a central authority that controls the network membership.	Necessity fo synchronization
Hu at al.	2004	Directional Antennas	Each pair of nodes determines the direction of received signals from neighbor; if directions match, relation is set	Not applicable t network withou directional antenna
Qian et al.	2005	Statistical Analysis	Identifying highest frequency link through analyzing relative frequency of each link appearing in obtained routes	Works only wit multipath on deman protocols
Khalil et al.	2005	LiteWorp	Instead of one-hop, two-hop routing information is obtained by nodes; now nodes know their neighbors' neighbor	Works only fo stationary networks
Lazos et al.	2005	Localization	Location Aware Guard Nodes (LAGNs) send hashed messages; if wormhole is present, a node detects inconsistencies in the message	Not applicable to mobil networks
Hu et al.	2006	Temporal Leashes	Timestamp given for packet	All nodes require tightl synchronized clocks
Weichao et al.	2006	End-to-end Leashes	Each intermediate node appends time and location information and receiver authenticates time and location information of a packet using symmetric key	Limitations of GP technology
Chiu et al.	2006	DelPHI protocol	protocol allows a sender to observe the delays associated with the different paths to a receiver. Therefore, a sender can check whether there are any malicious nodes sitting along its paths to a receiver trying to launch wormhole attacks. The obtained delays and hop count information of some disjoint paths are used to decide whether a certain path among these disjoint paths is under a wormhole attack.	Necessity to calculat delay between sourc and destination nodes
Van Phuong	2007	RTT	Each node in an established route computes the RTT between it and the destination and then sends this value back to the source node. The source node identifies wormhole based on the fact that RTT	Necessity to calculat RTT between sourc

t al.		approach	between two nodes with a wormhole link in between will be considerably higher than that between two real neighbors. This is another delay only detection method which may result in high false alarm rate when two legitimate neighbors suffer link congestion and have different intranodal processing speeds.	and destination nodes
Nait-Abdesselam t al.	2008	Proposed method	To pinpoint wormhole links before applying the detection mechanisms. If HELLO rep from a node is not reached before the timeout interval, the originator ranks the node as suspicious and stops communication with it until the end of wormhole verification process. In the verification phase the originator sends probing packets to all the suspicious nodes. However, both phases of this wormhole detection method depend on delay only mechanisms which may generate high false alarm rate.	Method depend on dela only mechanisms whic may generate high fals alarm rate.
Lee et al.	2008	TTL base approach.	Each node gathers information of its neighbors within two hops. Each newly joined node broadcasts an announcement which is valid until the next two hops. The requirement of maintaining two-hop neighbors, keyed hash and TTL limit the applicability of this method in a distributed system where exists a wide variety of participants.	Not applicable t wireless senso networks
Awerbuch et al.	2008	ODBSR	Proposed scheme uses the packet acknowledgement to detect packet dropping and then sends probe packets to identify the compromised nodes.	Overhead of Additiona packet (probe packets)
Yu et al.	2009	SRAC	Proposed a shared key to be maintained between the source and any other node along the route. Therefore, a node will receive multiple copies of the same packet from the source. After comparing multiple copies, it is possible to detect any missed or modified copies and identify the compromised nodes. Unfortunately, all these schemes are very complicated and only focusing on packet dropping or modification. If the compromised nodes are only interested in analysing traffic or spoofing, all these schemes fail.	Maintained shared ke between the source an any other node along th route
Chen et al	2010	Secure localization	proposed a secure localization approach based upon the conflicting set based resistant localization	Test Location
Modirkhazeni et al	2011	distributed network discovery approach	proposed distributed network discovery approach to mitigate wormhole effect	-

Vani et al	2011	Hybrid routing algorithm	Combines the methods of hop count, decision anomaly and neighbor list count methods for AODV protocol. The process depends upon hierarchical processing of nodes and their neighbors. They used the hop count present in the routing table of nodes, this will require that we need to store two copies of routing table of each node so that to keep track of previous hop counts.	-
Shin et al.	2012	Redundancy-Aggregation-RTT approach	Proposed routes redundancy and time-based hop calculation for wormhole attacks detection in MANETs. That consists of three phase which are routes redundancy, routes aggregation and round-trip-time calculation.	Not applicable t wireless senso networks
Sundararajan et al.	2013	BAIDS	Include hybrid negative selection algorithm (HNSA) detectors in the local and broad detection subsection to detect anomalies in ad hoc network. In addition to that, response will be issued to take action over the misbehaving nodes. These detectors employed in BAIDS are capable of discriminating well behaving nodes from attacking nodes with a good level of accuracy in a MANET environment.	applicable to mobile a hoc networks

I. CONCLUSION

Routing protocols in MANET are assailable because of the inherent design drawbacks. Secure routing has become a main concern for researchers as design of default MANET routing protocols considers a reliable environment. A particularly hazardous security attack that affects the MANET routing protocols, it is named the wormhole attack. Many researchers have used various methods to propose various kinds of detection and prevention mechanisms for wormhole attack. We surveyed present approaches to detect and prevent these attack. Finally, we've carried out a detailed comparative analysis of these methods according table III to their relative features and restrictions.

REFERENCES

i. 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; IEEE, 2013.

ii. Hu Y-C,PerrigA,Johnson D.Wormhole attacks in wireless networks. IEEE Journal on Selected Are as in Communications 2006; 24(2):370–80.

iii. Wang W,Bhargava B,Lu Y,Wu X. Defending against wormhole attacks in mobile ad hoc networks. In: Wireless communication and mobile computing; 2006.

iv. Capkun S, Buttyan L, Hubaux J-P.SECTOR: securetracking of node encounters in multi-hop wireless networks. In: ACM work shop on security of ad hoc and sensor networks(SASN);2003.p.21–32.

v. V Karthik Raju, K Vinay Kumar, "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks". IEEE International Conference on Computing Sciences, 2012;

vi. Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group; Jan 2004.

vii. Reza Fotohi, Shahram Jamali, Fateme Sarkohaki,"Performance Evaluation of AODV, LHC-AODV, OLSR, UL-OLSR, DSDV Routing Protocols", IJITCS, vol.5, no.10, pp.21-29, 2013. DOI: 10.5815/ijitcs.2013.10.03

viii. Benjamin J. Culpepper, H.Chris Tseng," Sinkhole Intrusion Indicators in DSR MANET", First International Conferenc on broadband networks IEEE 2004.

ix. Reza Fotohi, Shahram Jamali, Fateme Sarkohaki, Shahram Behzad,"An Improvement over AODV Routing Protocol by Limiting Visited Hop Count", IJITCS, vol.5, no.9, pp.87-93, 2013. DOI: 10.5815/ijitcs.2013.09.09

x. Qazi SH, Raad R, Mu Y, Susilo W. Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications; 36(2):582–592. 20113

xi. Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149.

xii. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad- hoc Networks: A Survey", In Proc. Of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.535-541.

xiii. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

xiv. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP Journal of Computer Science, vol. 11 no. 1, March 2012, pp. 1-12.

xv. Korbakorba A, Nafaa M, Ghanemi S, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks". IEEE International Conference on Computer Modelling and Simulation, 2013;

xvi. Y.C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," Proc. 2nd ACM workshop on Wireless security (WiSe '03), 2003, pp. 30-40,doi:10.1145/941311.941317.

xvii. S. Roy, S. Singh, S. and N. Debnath, "Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management", In Proceeding of IEEE Symposium on Computers and Communications, July 2008, pp. 537-542.

xviii. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96-97.

xix. Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

xx. Pradip M, Jawandhiy A, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, vol. 2 no. 9, 2010, pp. 4063-4071.

xxi. Ehsan H, Khan F, "Malicious AODV". IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012;

xxii. Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song,"Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Consumer Electronics, IEEE, May 2010, pp. 579-582.

xxiii. H.J. Kim and M.P. Jon, "Detecting selfish behavior in a cooperative commons," Proc. Third IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks DySPAN, Chicago, Illinois, Oct. 2008, pp. 1-12, doi: 10.1109/DYSPAN.2008.22

xxiv. V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

xxv. H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

xxvi. R. Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010.

xxvii. S. Capkun, L. Buttyan, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multihop Wireless Networks," *Proc. ACM Wksp. Sec. of Ad Hoc and Sensor Networks*, Fairfax, VA, Oct. 2003.

xxviii. L.Lazos, R. Poovendran, "Serloc: Secure Range-IndependentLocalization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

xxix. L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference, 2005.

xxx. I.Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

xxxi. L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

xxxii. Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

xxxiii. W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

xxxiv. H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," *Proc. Int'l. Symp. Wireless Pervasive Comp.*, Phuket, Thailand, Jan. 2006.

xxxv. T. Van Phuong, N. T. Canh, Y.-K. Lee, S. Lee, and H. Lee, "Transmission time-based mechanism to detect wormhole attacks," in Proc. 2nd IEEE Asia-Pacific Service Computing Conference 2007, pp. 172–178.

xxxvi. F. Nait-Abdesselam, "Detecting and avoiding wormhole attacks inwireless ad hoc networks," IEEE Comm. Mag., pp.127–133, Apr. 2008.

xxxvii. Lee, G., J. Seo, and D. Kim. *An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks*, in Proc. ISA2008.

xxxviii. B. Awerbuch, R. Curtmola, D. Holmer, *et. al.*, "*ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks*". ACM Trans. Inf. Syst. Secur., 2008. 10(4): p. 1-35.

xxxix. M. Yu, M.C. Zhou, and W. Su, "*A secure routing protocol against byzantine attacks for MANETs in adversarial environments*". IEEE Transactions on Vehicular Technology, 2009. 58(1): p. 449-460.

xl. Honglong Chen , Wei Lou , Xice Sun , Zhi Wang, A secure localization approach against wormhole attacks using distance consistency, EURASIP Journal on Wireless Communications and

xli. Networking, 2010, p.1-11, April 2010

xlii. Modirkhazeni, A.; Aghamahmoodi, S.; Modirkhazeni, A.; Niknejad, N.; , "Distributed approach to mitigate wormhole attack in wireless sensor networks," Networked Computing (INC), 2011 The 7th International Conference on , vol., no., pp.122-128, 26-28 Sept. 2011

xliii. A.Vani, D.Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc

xliv. Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), 2011, Vol. 3 No. 6, pp. 2377-2384, June 2011

xlv. L.Lazos, R. Poovendran, "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation ", ICT Convergence (ICTC), 2012 International Conference on, pp. 781-786, 2012.

xlvi. T. V. P. Sundararajan, S. M. Ramesh, "Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET", Wireless Netw, 2013

xlvii. Ning Song, Lijun Qian, and Xiangfang Li. Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach. In the proceedings of the 19th IEEE international parallel and distributed processing symposium (IPDPS'05); 2005.

xlviii. Hon Sun Chiu, King-Shan Lui. DelPHI: wormhole detection mechanism for ad hoc wireless networks. In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.

xlix. Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, An approach to mitigate wormhole attack in wireless ad hoc networks. In the proceedings of the international conference on information security and assurance; 2008. pp. 220–5.

l. Xu Su and Rajendra V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. In the proceedings of the IEEE international conference on communications; 2007. pp. 1136–41.

li. Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks. In the IEEE securecomm and workshops; 2006. pp. 1–12

lii. Xia Wang and Johnny Wong, An end-to-end detection of wormhole attack in wireless ad-hoc networks. In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007.

liii. Petrova, K., &Wang, B. (2011). Location-based services deployment and demand: a roadmap model. Journal of Electronic Commerce Research, 11(1), 5–29.

liv. Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. Journal of Electronic Commerce Research, 11(1), 31–74.

lv. Zhou, T. (2013). An empirical examination of user adoption of location-based services. Journal of Electronic Commerce Research, 13(1), 25–39.

lvi. Hu, L., & Evans, D. (2004). Using directional antennas to prevent wormhole attacks. In Network and distributed system security symposium (pp. 131–141).

lvii. Gorlatova MA, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano. Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. In the proceedings of the IEEE conference on military communications; 2006.

lviii. Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F, Magdy S. El-Soundani. Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme. In the proceedings of the IEEE international conference on availability, reliability and security; 2008. pp. 636–41.

lix. Xia Wang, Intrusion detection techniques in wireless ad hoc networks. In the proceedings of the IEEE international computer software and applications conference; 2006.

lx. Su, M.-Y. (2009). WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Journal of Computers & Security, 29(2), 208–224.

lxi. Xu Su and Rajendra V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. In the proceedings of the IEEE international conference on communications; 2007. pp. 1136–41.

lxii. Mahajan V, Natu M and Sethi A. ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS. IEEE; 2008.

Authors Profiles

Reza Fotohi received his B.Sc. in computer engineering from Shabestar University of Applied Science And Technology, Tabriz, Iran, in 2009, and his M.Sc. in Computer Engineering from Islamic Azad University, Germi branch, Ardabil, Iran, in 2013. His research interests include wireless networks, mobile computing and combinatorial optimization.

Shahram Jamali received his B.Sc. degree in Computer Engineering from Amirkabir University, Tehran, Iran, in 1999, his M.Sc. degree in Architecture of Computer Systems from Iran University of Science & Technology (IUST), Tehran, Iran, in 2001, and his Ph.D. degree in Architecture of Computer Systems in 2008. He is currently Associate Professor of Computer Engineering at University of Mohaghegh Ardabili (UMA). His research interests include Congestion Control in computer networks, Self-managing Computer Systems, Biologically-inspired Networking and Load balancing in Grid environment.