DOI: 10.21917/ijct.2016.0209

A SURVEY ON DELAY AND NEIGHBOR NODE MONITORING BASED WORMHOLE ATTACK PREVENTION AND DETECTION

Sudhir T. Bagade[1] and Vijay T. Raisinghani[2]
[1]*Department of Computer Science and Technology, Usha Mittal Institute of Technology, India*
E-mail: bsudhiran@ieee.org
[2]*Department of Information Technology, School of Engineering, Narsee Monjee Institute of Management Studies, India*
E-mail: rvijay@ieee.org

Abstract

In Mobile Ad-hoc Networks (MANET), network layer attacks, for example wormhole attacks, disrupt the network routing operations and can be used for data theft. Wormhole attacks are of two types: hidden and exposed wormhole. There are various mechanisms in literature which are used to prevent and detect wormhole attacks. In this paper, we survey wormhole prevention and detection techniques and present our critical observations for each. These techniques are based on cryptographic mechanisms, monitoring of packet transmission delay and control packet forwarding behavior of neighbor nodes. We compare the techniques using the following criteria- extra resources needed applicability to different network topologies and routing protocols, prevention/detection capability, etc. We conclude the paper with potential research directions.

Keywords

Ad-hoc Network, Secure Routing, Wormhole Attack, Hidden Wormhole, Exposed Wormhole

1. INTRODUCTION

Mobile Ad-hoc routing protocols are vulnerable to routing attacks like *wormhole*, *black-hole*, *rushing*, *replay* and *flooding* [1]. In this paper we focus on wormhole attacks. The Fig.1 shows a typical wormhole attack scenario. Nodes named *X* and *Y* creates the wormhole. The thick dashed arc in the figure indicates the transmission range of the wormhole nodes. A wormhole receives packets at one point in the network, *tunnels* them to another point in the network, and then replays them into the network from the other end point. These colluding wormhole nodes may use a fast out-of-band channel (either wired or wireless) or in-band-channel [2] to pass the packet to another point in the network. When nodes behave in a non-malicious manner, that is, they forward the correct routing packets to other nodes in a standard way; the existence of tunnels is actually beneficial because it increases the total capacity of the network [3]. However, an attacker might create a wormhole with a malicious intention. Such a wormhole could be used to analyze, modify or drop all or selected packets. One of the techniques used by the wormholes to attract traffic is to advertise lesser number of hops in their route replies, thus creating a fake shortest path passing through them. An attack of this kind would lead to degradation in the performance of network routing and/or data transmission. The metrics for measuring the degradation in performance would be delay in transmission, packets dropped, number of fake route requests, etc.

In literature, two types of wormhole attacks have been described- *hidden* and *exposed*. This categorization is based on the visibility of the wormhole on the routing path.

Hidden channel wormhole- A hidden wormhole attack is defined as an attack in which two or more nodes collude in the routing process, without being *visible* on the path between source and destination nodes. The nodes hide their presence by manipulating the mechanism of IP-in-IP. This type of attack is also termed as *external channel* or *traditional attack.*

Exposed channel wormhole- Exposed channel wormhole attack is defined as an attack against routing protocols in which two or more malicious nodes collude and are visible on the routing path. Once these nodes get included in the shortest path they can fabricate, modify, or misroute packets in an attempt to disrupt the routing services [4]. This type of attack is also termed as *internal* or *byzantine attack.*

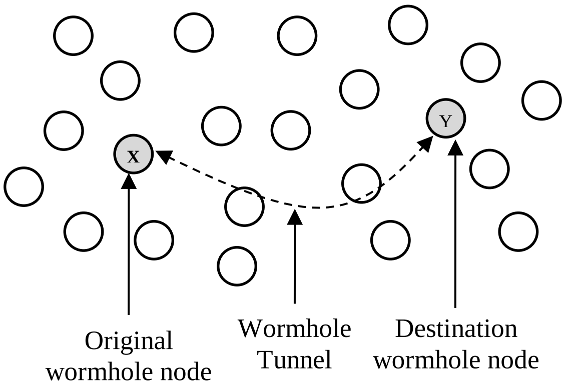


Fig.1. Typical wormhole attack

Initially, when ad-hoc routing protocols such as Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) and Temporally Ordered Routing Algorithm (TORA) [1] [5] were developed, no security aspects were considered. Later, secure routing protocols like Authenticated Routing for Ad-hoc Networks (ARAN) [6], ARIADNE [7], Unobservable Secure Routing protocol (USOR) [8], Secure-AODV [9], Security Aware Routing (SAR), Secure-OLSR [10], and Secure Efficient Ad-hoc Distance Vector (SEAD) [11] were developed to address the threats to the ad-hoc routing protocols. These secure routing protocols use symmetric/asymmetric cryptography or one way hash chain mechanisms [12] to protect packet data and header from unauthorized access. However, these secure protocols relying on cryptographic mechanisms cannot prevent or detect wormhole attacks, as the wormhole attacks can be launched without accessing message contents.

To protect ad-hoc networks from wormhole attacks, the first and key step is prevention of a wormhole [3] and the next important step is detection. In this paper, we survey wormhole prevention and detection techniques. Prevention techniques are based on strong cryptographic mechanisms [3] [13] [14] while detection techniques are based on the measurement of packet transmission delay [13] [14] [15] [16] or monitoring of packet forwarding behavior of neighbor nodes [2] [4] [17] [18]. In case of the cryptographic approach, each packet is encrypted by using the symmetric or asymmetric keys and each node is authenticated using hash code and digital signature. Using this approach, wormholes can be prevented because the colluding nodes do not have the keys needed to participate in the routing process. In case of the approach measuring packet transmission delay, a sender verifies whether per hop delay in transmitting a packet or end to end delay on a path are below some computed threshold. If the delay is higher than the threshold, then the sender concludes that a wormhole exists on the path. In case of the approach wherein neighbor node forwarding behavior is monitored, the sender as well as each intermediate node checks whether its neighbor node forwards a packet received by it, within a certain time limit.

The rest of this paper is organized as follows. In section 2, we present the overview of secure routing protocols. Section 3 reviews the algorithms for prevention and detection of hidden and exposed wormholes. In section 4, we compare the wormhole prevention and detection methods using some key criteria and analyze the methods surveyed. We conclude the paper along with directions for further research in section 5.

2. OVERVIEW OF SECURE ROUTING PROTOCOLS

In absence of some sort of security mechanism to protect data control packets, routing protocols are vulnerable to malicious attacks such as spoofing, man in the middle attack, replaying, black hole, denial of service, rushing and wormhole attacks [1]. In order to avoid these attacks, secure routing protocols using hash functions, hash chains and cryptographic solutions have been proposed in ad-hoc routing literature [3] [6-12]. Below we discuss some of these secure routing protocols and show how these algorithms are vulnerable to wormhole attacks.

2.1 AUTHENTICATED ROUTING FOR AD-HOC NETWORKS (ARAN)

Authenticated Routing for Ad-hoc Networks (ARAN) [6] is based on AODV in which each node has a certificate signed by a trusted authority. ARAN assumes public key infrastructure for end to end authentication and neighbor node authentication, in route discovery. Replay attacks are prevented by using time stamps in the packet. Similarly, spoofing attack is prevented by the source node by using a digital signature and including a nonce in the packet. These attacks are prevented because each packet is checked and processed based on the latest time stamps and freshness of a nonce.

Problems: Every node that forwards a route discovery or a route reply message must also sign it, which is not energy efficient and causes the size of the routing messages to increase at each hop. Also, the protocol is prone to hidden wormhole attack, since the colluding node at one end can forward the packet to the other colluding node using encapsulation, without the need for a digital certificate. The other colluding node can then replay the packet at the other end of the wormhole. This is sufficient to disrupt the ad hoc network routing.

2.2 ARIADNE

ARIADNE [7] is a secure on-demand routing protocol based on Dynamic Source Routing (DSR) [5] and Timed Efficient Stream Loss-tolerant Authentication (TESLA) [6] [13]. ARIADNE prevents node compromise and relies on symmetric key cryptography. It requires time clock synchronization among all nodes in the ad-hoc network. With each packet transmitted by the source node, a cryptographic key is sent along with the sending time, to the destination. This key expires after a certain set time. Due to this reason hidden wormhole attack is not possible as the key will be invalidated if not used within the predefined time by the receiver. ARIADNE authenticates routing messages using shared secret keys between all pairs of nodes along the path or between source and destination nodes.

Problems: ARIADNE protocol is vulnerable to exposed wormhole attack on the selected path because intermediate nodes can read the keys. There is no feedback to the source node about the behavior of intermediate nodes. Information whether intermediate nodes are forwarding the packets or not, or the reason for dropping packets is not given to source node.

2.3 UNOBSERVABLE SECURE ROUTING PROTOCOL (USOR)

In Unobservable Secure Routing protocol (USOR) [8], the authors have described a cryptographic mechanism to encrypt data as well as header part of the packet while transmitting from source to destination. The protocol uses group signature, to ensure complete protection of each packet from intermediate nodes. Group signature is an encrypted digest of the node identifiers which are on the path in use. The packets are, thus, unobservable and cannot be linked to each other by any intermediate node while being forwarded towards the destination.

Problems: Even with secure routing, the authors point out that wormhole attack is still possible. This is due to the fact that in case of hidden wormhole it’s a matter of just copying the packet without immediate deciphering of the packet and replaying it at distant location using a colluding node.

2.4 SECURE AD-HOC ON DEMAND DISTANCE VECTOR (S-AODV)

Secure Ad-hoc On demand Distance Vector (S-AODV) [9] is a secure version of AODV [1] protocol. A one way hash chain is used to authenticate the hop count of Route Request (RREQ) and Route Reply (RREP) messages to verify that hop count is not decremented by an attacker. S-AODV assumes public key infrastructure and uses digital signatures to protect the integrity of the non-mutable data in control messages. If an intermediate node *i* have cached the route to the destination then it sends a route reply to the source node. After receiving the route information, the source node sends further route request to the immediate next neighbor *i*+1 of the intermediate node *i*. The intermediate node *i* is trustworthy, if the route reply from the (*i*+1)th node includes the intermediate node *i* in the route information. Using this approach, S-AODV detects a single node hidden wormhole or black-hole.

Problems: S-AODV fails to detect a hidden node wormhole attack if two or more malicious nodes are colluding as the *i*th and (*i*+1)th node.

2.5 SECURE OPTIMIZED LINK STATE ROUTING PROTOCOL (S-OLSR)

Secure Optimized Link State Routing protocol (S-OLSR) [10] uses hash function and digital certificates to protect the routing packet and for authentication of the neighbor node respectively. Each node is equipped with public/private key pair. S-OLSR can detect hidden wormhole in the following manner. Node A determines whether node *B* is an immediate neighbor or not. A sends a HELLO message to *B*. A measures the time taken (*t*) for the message to reach *B* and uses it to compute the distance (*L*) to *B*.$L = t*c$, where c is speed of light. If *R* is the radius of coverage of node A and *L*>*R*, then it is assumed that a wormhole exists on the path to B.

Problems: We believe S-OLSR cannot detect hidden or exposed wormhole if it exists well within the coverage radius of A. Since, in this case *L*<*R*.

Table.1. Summary of secure routing protocols

Secure Routing Protocol	Routing protocols on which they are applied	Security mechanisms used	Wormholes not detected by the protocol
ARAN [6]	AODV	Public key cryptography and digital signature	Hidden
ARIADNE [7]	DSR	Symmetric key cryptography and TESLA [6] [13]	Exposed
USOR [8]	Reactive routing protocols	Symmetric cryptography, group signatures and ID based encryption.	Hidden
SAODV [9]	AODV	Asymmetric key infrastructure using digital signature and one way hash chains	Hidden
SOLSR [10]	OLSR	Hash functions and digital certificates	Exposed
SEAD [11]	DSDV	No cryptographic operations, only one way hash functions to check authenticity of messages.	Hidden and Exposed

2.6 SECURE EFFICIENT AD-HOC DISTANCE VECTOR (SEAD)

Secure Efficient Ad-hoc Distance vector (SEAD) [11] is based on Dynamic Sequenced Distance Vector (DSDV) [5] proactive routing protocol. Designed to overcome Denial of Service (DOS) and flooding attacks. A one way hash function is used to check the authenticity of the routing update message received from a node.

Problems: SEAD cannot avoid hidden or exposed wormhole if two or more attackers collude because it does not use a cryptographic mechanism. The hash of the update message is unsigned. The attacker may use the same sequence number of the recent routing update message and can mount impersonation or replay attack. If IP spoofing is used by an attacker then it may not be detected. In table 1 we summarize the review of secure routing protocols.

In this section, we discussed secure routing protocols and their vulnerability to wormhole attacks. In the next section, we review the mechanisms to prevent and detect wormhole attacks.

3. LITERATURE SURVEY

Wormhole attacks need to be prevented, detected and acted upon, if present in an ad-hoc wireless network. We first discuss the methods for wormhole prevention and then we present the methods for wormhole (hidden and exposed) detection.

3.1 METHODS FOR PREVENTING WORMHOLE ATTACKS

H. Pai and Wu [3], propose prevention of wormhole (PW) protocol based on advanced encryption standard (AES) and elliptic curve cryptography (ECC) to prevent both hidden and exposed wormhole attacks for a mobile commerce application. The system has three key entities bank, merchant and customers (nodes). The bank holds the cryptographic keys, certificates and other parameters required for onion encryption. The customers acquire their identity and certificate from the bank, using secure socket layer communication. Also, the customers get the bank and merchant's public keys, certificates and a group key from the bank. A malicious node cannot access the bank to get this information. Each customer derives its own secret key using the witness (number) and certificate. Route discovery packets between a source node, intermediate nodes and merchant node are encrypted using the group key. The group key is used to encrypt the identity of source node and each intermediate node. Each intermediate node along the path signs the packet using its secret key and encrypts this information using the merchant's public key. After receiving the route request, the merchant applies its signature and returns the routing reply message to the source node. Hidden and exposed wormhole is prevented because wormhole attacker does not possess the cryptographic keys which are necessary to perform *onion encryption*.

Observations: ECC based onion encryption and AES based group key provides very strong cryptographic mechanism in the PW protocol. However, if a node is compromised at the beginning itself, then this mechanism would not be able to prevent a hidden wormhole attack. Hidden wormholes could do malicious activity like packet dropping which is not addressed by the proposed method.

Y. Hu proposed packet leashes in [13] to protect against wormhole attacks at MAC layer. A leash is nothing but the time restrictions applied on a packet to decide its validity. Authors proposed two types of leashes: geographical leashes and temporal leashes. Geographical leash comprises of sending time and location of a node which is appended into the packet. This leash in the packet decides the maximum allowed distance from the sender node. At the receiver node, if a packet received does not violate the leash condition, the receiving node assumes that the network path is wormhole free, else the packet is discarded. In temporal leash, upper bound on time is computed using the difference between packet sending time and packet receiving time. If the time taken by a packet is greater than the upper bound between sender node and receiver node then the receiver assumes that a wormhole exists and discards the packet.

Observations: Transmission of extra information like location and time in the packet leads to increased traffic overhead. Global positioning system (GPS) is required in case of geographical leash to track the location of nodes. This method is not energy efficient because of use of GPS system for location tracking. If a wormhole is created using a low delay channel, then the packets may reach the destination faster. In this case, the wormhole would remain undetected since the temporal leash will not be violated.

R. Matam and Tripathy [17] propose a WRSR: Wormhole Resistant Secure Routing for Wireless Mesh Networks to defend against hidden and exposed wormholes during route discovery process. The protocol works in a wireless mesh network and employs the mechanism of neighborhood connectivity information. Each node maintains the list of its 2-hop neighbors. A wormhole is detected by a node if it receives a RREQ packet which has not traveled to it through the valid 2-hop neighbors, in its list. Further, WRSR validates the paths by checking alternative sub-paths. Wormholes would shorten the alternative sub-paths.

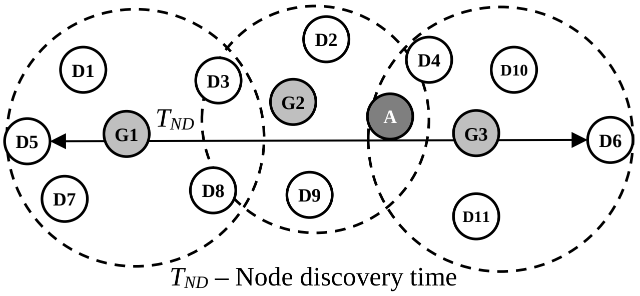
Observations: WRSR relies on the assumption that alternative sub-paths exist in a dense network. A wormhole would reduce the natural length of longer sub-paths. Thus if only shorter length sub-paths are visible then a wormhole probably exists. In case the wormhole itself is of short-length then the probability of detecting it would be low.

3.2 METHODS FOR DETECTING HIDDEN WORMHOLE ATTACK

In this section we discuss techniques for the detection of hidden wormhole. Since hidden wormholes do not participate in routing, detecting them can be done through indirect means such as delays introduced by them on a path or changes in hop count.

Khalil et al. [2] proposed LITEWORP as a secure ad-hoc neighbor discovery and control traffic monitoring method to detect the wormhole attack. This method assumes static topology and redistribution of pair of keys for secure communication. It is based on neighbor node monitoring, and the assumptions that an attack can be launched by an external node (without keys) or internal node (with keys).

As shown in the Fig.2, some nodes in the network are designated as guard nodes, denoted by G1, G2 and G3. The malicious node is denoted by A. Nodes numbered D1 to D11 are normal nodes. Dotted circles denote the coverage and transmission range of guard nodes. Guard nodes are statically deployed in the network. It is assumed that together the guard nodes can monitor all the nodes in the network. If a node behaves maliciously i.e. drops or fabricates a control packet, then the guard node informs all neighbors of the malicious node. The guard node maintains a *malicious counter* for all nodes in its proximity. A node is marked as malicious, if its malicious activities counter crosses a predefined threshold.



T_{ND} – Node discovery time

Fig.2. Malicious node detection and isolation

Node discovery time (T_{ND}) is the time required to discover all the 1-hop and 2-hop neighbors before the time required to compromise any of these nodes.

Observations: LITEWORP does not require any special hardware or tight clock synchronization among nodes. Authors have not discussed whether the method is applicable to any specific routing algorithm and type of wormhole. The problems in this algorithm are: the overhead of control message exchange among neighbor nodes and guard nodes. Due to this more battery power would be consumed. If a genuine node is overloaded with control packets, it may drop some packets and this could result in it being marked as a malicious node.

Su and Boppana [14] use the concept of flooding of RREQ and RREP packet to detect a wormhole. It is designed with secure ARIADNE protocol [7]. Two techniques are used to detect wormholes. First, *destination statistical profiling* that detects the presence of a wormhole by computations at the destination node, and second, *source statistical profiling* that detects the presence of a wormhole by computations at the source node. In the first technique, the RREQ packet received at the destination with a new sequence number is considered as a legitimate request from the source. Using time stamps and the number of hops information in the RREQ the destination computes the Route Request Hop Time (RHT). If for any duplicate RREQ the new RHT is greater than the first RHT, then it is assumed that the wormhole is present on that path. Similarly, in second method, the *source statistical profiling* is performed on RREP packet received by source node. Authors have adapted the Retransmit Timeout (RTO) calculations used by TCP, which captures both the average and deviation of round trip time of a connection. Source node computes the average delay between the hops using RREP packet. When the source receives a RREP packet, it computes Route Discovery Hop Time (RDHT) as the route discovery time divided by the received hop count in RREP. If RDHT is more than the pre-computed average delay, then the path is assumed to have a wormhole.

Observations: If first RREQ or RREP packet itself traveled through wormholes, then this technique may fail to detect the wormhole. Due to traffic congestion some genuine nodes could be perceived as wormholes, so there is a chance of false positives. Intermediate nodes are not participating in detection of a wormhole, so determining the location of wormhole is not possible.

F. Nait-Abdesselam [15] measures the response speed of neighbor nodes to identify suspicious links. To detect a wormhole link, the source node broadcasts HELLO messages to discover its neighbors. After sending *n* HELLO messages, one special HELLO Request is sent and expiry timeout is set. Timeout is set using formula: Timeout= $2R/V + T_{\text{proc}}$, where, R: maximum transmission range of each node, V: is propagation speed of signal (e.g. speed of light), T_{proc}: is packet processing time and queuing delay within a node. Each neighbor node replies with a HELLO Reply message to the source node. On a link, if the reply packet is received after the timeout, then that link is marked as a suspicious link. Further, for confirmation of a wormhole on the suspicious link, two new messages are introduced into the protocol, that is *Probing* and *ACK-prob* (reply) messages. These messages are used to confirm the presence of a wormhole link. Once again, the originator of *Probing* packets checks whether the *ACK-prob*, from each of its neighbors, arrived within the required timeout.

Observations: Using this method any legitimate link could be marked as a wormhole link since delay can be caused by traffic congestion also. Control messages are sent without any cryptographic mechanism, so any malicious node may read the packet header and use IP spoofing to prevent its detection. If the link to a wormhole node takes lesser time compared to the wormhole free link, then the wormhole cannot be detected by this method.

Z. Shi et al. [16] propose a wormhole attack resistant, Secure Neighbor Discovery (SND) scheme, for a centralized 60GHz directional wireless network. The whole network is divided into 8 sectors, using directional antennas. One network controller (NC) exists at the center of the network. Hidden wormhole is detected in three phases, namely the NC broadcast phase, response/authentication (RA) phase and the time analysis phase. In the first phase NC broadcasts *Hello* messages to its neighbors, in a specific sector. In the second phase, all neighbor nodes, within the sector, respond to the *Hello* messages by sending *directional authentication* frame to the NC. When the NC gets the frame, it calculates the angular difference in the current direction of NC and that of the node which has responded. If the angular difference is not within a predefined threshold then a wormhole is assumed to be present. In third phase, the NC does time analysis to detect wormholes beyond the radius of communication. If a malicious node is outside the communication range of the NC, then its authentication frame would arrive later as compared to that of nodes within the communication range.

Observations: The above mechanism is applicable to only to 60GHz directional and centralized wireless network. It would fail to detect a wormhole in a distributed wireless network with omni-directional antennas. Only single node hidden wormhole is detected.

Chen H et al. [18] propose a label based secure localization scheme which use DV-hop localization procedure to detect the wormhole attack. In wireless sensor network there are two types of nodes, that is beacon and sensor nodes. Each beacon node estimates minimum hop-count to each of the beacons using distance vector routing mechanism. Each node floods HELLO message containing nodes location, id and hop count information into the network. When other beacon nodes hear this HELLO message they also put their id into the message and increase the hop count. This way all the nodes in the network estimates the minimum hop-count to each of the beacons and their positions. Using this information, the beacon node estimates the average distance per hop called as hop-size in the network. Now the sensor nodes calculate its distance to each of the beacon nodes by using its hop-count to beacon node and the average hop-size.

The main idea of the proposed scheme is to mark either beacon and sensor nodes with labels like wormhole node or no wormhole node if the respective node violates the communication properties. This marked label list is maintained by each neighbor node. If a particular communication path is going through the wormhole nodes, then such a link is marked as a wormhole link and debarred from future communication.

Observations: The proposed technique may not detect the wormhole nodes correctly if the transmission radii of the nodes are different because then the estimation of hop-size would be different for each sensor node. This results into more false positives and negatives.

W. Wang [19] proposed Interactive Visualization of Wormhole (IVoW), which provides visual approach for the detection of multiple wormholes in large scale, dynamic wireless network. First, every pair of nodes that are within the radio range will estimate the distance between themselves. This pair-wise distance is used by IVoW to construct the distance matrix among neighboring nodes. The classical shortest path algorithm, such as Dijkstra’s algorithm is applied on distance matrix to calculate shortest distance between every pair of node. Now, a mechanism called Multi-Dimensional Scaling (MDS) is used to reconstruct the distance matrix whenever network topology changes. MDS is used to detect the fake neighbors as follows. In the reconstructed matrix, if a pair of nodes is far away from each other in the previous distance matrix and suddenly become neighbors in this reconstruction then the link between them is detected as a wormhole link.

Observations: IVoW and MDS together handle large number of moving nodes and detect multiple wormholes using node connectivity information. If a non-malicious node moves close to the far away recipient node then non-malicious node is also detected as a wormhole node.

F. Shi et al. [20] proposed a method for detection and location of hidden wormhole. It is based on computing the number of hops required to reach the destination and actual hop count received in the RREP packet. It works in two phases: detection phase and location phase. In the detection phase, the source sends the RREQ packet and starts a timer. On the receipt of RREP, the distance to the destination is calculated as the round trip time divided by 2. The per-hop time is estimated as per the node placement and topology by source node. The hop count to the destination is computed as the distance divided by one hop time. If the received hop count in RREP is less than the calculated hop count then a wormhole is assumed to exist on the path. After detection of the wormhole the location phase starts, in which trace packets are sent by the source node to each intermediate node along the path. Each intermediate node i has to reply to the source the hop count it has determined up to the destination node along with the id of (i+1)th node. Hop count reported by the (i+1)th node must be one higher than that reported by the ith node. Otherwise the ith and (i+1)th nodes are assumed to be the wormhole nodes.

Observations: The challenge in this algorithm is that if the node density is higher or if the traffic is heavy then the routing performance tends to be poor because hop count is estimated for each RREQ and RREP. Further, the delay could be due to congestion. Hence, a congested path may be detected as a wormhole. In this case, the location phase could be initiated unnecessarily, due to which the overall performance of routing process would degrade.

3.3 METHODS FOR DETECTING EXPOSED WORMHOLE ATTACK

There are many techniques suggested in literature to thwart exposed wormhole attack. In exposed wormhole, nodes are actually participating in route discovery and data transmission process. Some of the techniques can detect both hidden and exposed wormholes. The techniques primarily focus on monitoring node behavior during packet forwarding. We discuss some of these techniques below.

M. Yu [4] have proposed Secure Routing Against Collision (SRAC) using public key cryptographic mechanism and shared keys which are distributed at the time of node deployment. MD5 algorithm is used for signature and node authentication. The source sends a plain text message along multiple disjoint paths to the destination node. Each node along a path signs the message and sends it to the next node. The destination node compares the messages received along these multiple paths. If any difference between the messages is found then the node that has made changes or modification is identified using the signatures and assumed to be a wormhole node.

Observations: The problem with this technique is the overhead of sending multiple signed messages. Each destination node is required to receive *n* copies, one along each of the *n* paths to detect modifications in the packet. This increases communication overhead at the destination. Wormhole detection would be difficult if the network is sparse and the paths are not disjoint.

In [21], On Demand Secure Byzantine Resilient Routing (ODSBR) protocol is designed and focuses only on packet dropping as the criteria for exposed wormhole detection. It uses symmetric/asymmetric key mechanism to secure the communication. In ODSBR, each node assigns a weight to each link. For every successful packet delivery, the link weight is not increased and for every unsuccessful packet delivery the link weight is doubled. A link with higher weight is treated as unreliable and avoided by the sender. A link with lower weight is considered reliable and could be chosen by the sender for packet transmission. The algorithm assumes that some packet losses will occur during packet transmission. An appropriate link weight is used to set the packet loss threshold. A *fault* is defined as a loss rate greater than or equal to the set threshold. To acknowledge packet receipt, each node in the route discovery process sends an authenticated *ack* to the source within a set timeout, using hash function for message authentication code (HMAC). After the detection of a faulty link, *Prob* packets are sent by the source node on the faulty link to each intermediate node for the detection of wormhole.

Observations: ODSBR may not detect the wormhole in the case when instead of packet dropping by a malicious node it forwards the packet to its colluding node and then colluding node could analyze the packet content or replay it. In this technique, a non-malicious node may also be classified as a wormhole if traffic congestion occurs at that node.

3.4 METHODS FOR DETECTING HIDDEN AND EXPOSED WORMHOLE ATTACK

In this section we review the mechanisms that detect or prevent both, hidden and exposed wormhole attacks.

H.S. Chiu et al. [22] have proposed the Delay per Hop Indicator (DelPHI). It can detect both hidden and exposed wormhole attacks. In the original AODV protocol the destination node sends RREP to the sender node only for the first RREQ received and subsequent RREQ will be dropped at the destination. In DelPHI, AODV is modified such that, all RREQ are forwarded and the destination node replies to all RREQs. Source calculates the per hop delay for every disjoint path. The delay and number of hops for each route is calculated and the average Delay Per Hop (DPH) along each route is computed as the RTT divided by twice the hop count. The route having a DPH higher than the average is assumed to have wormhole link.

Observations: The authors have only considered equally placed nodes and have not analyzed the mechanism for general deployment of nodes. This mechanism can detect the existence of a wormhole but it cannot detect the location of the wormhole. Wormhole cannot be detected if the delay through the wormhole is less than or equal to per hop pre-computed average delay.

Wormhole Attack Prevention (WAP) [23] detects hidden and exposed wormholes. It considers dynamic source routing (DSR) as the routing protocol. WAP does not require any special hardware or clock synchronization. Wormhole attack prevention (WAP) assumes bi-directional links and is based on neighbor node monitoring. For detecting hidden wormhole, node A sends RREQ packets and starts wormhole prevention timer (WPT). The WPT considered as the maximum amount of time required for a packet to travel from a node to a neighbor node and back. When node B receives the RREQ packet it should broadcast the RREQ immediately. This broadcast is also heard by node A. A check whether the RREQ from B is received within expiry of WPT. If A receives the message after WPT expires, it suspects B or B's next node to be a wormhole node. Wormhole prevention timer is computed using formula 2*TR/Vp, where, TR is the transmission range of a node. Vp is the propagation speed. For detecting exposed wormhole, the source node first computes the delay per hop (DPH) using the formula DPH= (Tb – Ta)/hop-count, where Ta is the time at which the RREQ was sent, Tb is the time at which RREP message is received and hop-count is the count received in RREP message. If DPH > WPT, then the presence of wormhole is assumed on the path.

Observations: Using the WAP algorithm it is hard to pinpoint the location of the wormhole because the delay per hop is an average value for a path. Processing delays at nodes are not considered in the per hop delay calculation of WPT. If the wormhole link takes lesser time as compared to normal transmission link, then the wormhole would remain undetected.

T. Pham [24] proposed a statistical wormhole attack detection approach in Delay Tolerant Network (DTN) [25] which uses store-and-forward routing mechanism. The network deploys the special nodes in the network called as infrastructure nodes. These nodes are responsible for a collection of neighbor count and detection of wormhole. Wormhole detection method is divided into two phases: training and testing. Initially, in training phase, infrastructure nodes estimates the average maximum neighbor count when there is no wormhole present in the network. In testing phase, again the information node computes the average neighbor count. If the ratio between the current neighbor count and average neighbor count estimated during training phase is greater than the set threshold then the wormhole is assumed to be present in the network.

Observations: Proposed method is simple and relies on the computation of neighbor count using infrastructure nodes. However, authors assume that initially, there is no wormhole attack till the training period. If the wormhole is present during training period then whole mechanism would fail and detection of wormhole may be difficult.

Above we have reviewed the papers specifically related to the delay and neighbor node monitoring based mechanisms. In literature, other proposals exist to defend against a wormhole attack, which is discussed below.

The mechanism proposed by Maheshwari in [26] is based on node connectivity information gathered in unit disk graph (UDG) model. This technique requires strict constraint on the network topology.

Wormhole Resistant Hybrid Technique (WRHT) is proposed in [27], uses the combination of packet drop probability and time delay probability to detect the wormholes in sensor networks. If the congestion occurs on the routing path then the technique may fail to detect the wormholes.

L. Chen [28] proposed a secure routing scheme called Single Trip Detection Mechanism (STDM) in wireless mesh networks to detect and isolate the hidden wormhole nodes. Timed colored petri net tool is used to model and verify the effectiveness of STDM. The detection takes place at intermediate and/or at destination nodes during the route discovery phase. So the detection is quicker as compared to other round trip time based mechanisms.

In [29], H. Chen proposed Secure Localization scheme Against Wormhole attacks (SLAW) based on the concept of conflicting sets. It has three types of nodes: sensors, locater and wormhole nodes. Sensor nodes are stationary or mobile nodes responsible for the actual communication. Locater nodes are stationary in the network and are responsible for providing a location to the sensor node when requested. Sensor node periodically sends the location request messages to the neighboring locater nodes. Locater node generates the conflicting set by detecting abnormalities in terms of massage exchange between sensor node and the locater nodes. Conflicting sets are nothing but the vector contains the locater's list (wormhole nodes) who does not follow route reply time and location information. The conflicting set is provided to the sensor nodes and using this set a secure communication takes place by avoiding wormhole nodes listed in conflicting sets. Scheme assumes that a sensor node cannot be a wormhole node. Proposed method works well with this assumption, however if the congestion occurs at locater node then false alarm rate would increase. A locater node relies on GPS to detect their location information.

In this section, we presented the survey on wormhole prevention and detection techniques. In the next section, we compare the techniques using various parameters.

4. COMPARISON OF WORMHOLE PREVENTION AND DETECTION ALGORITHMS

The techniques are compared using the following criteria: 1) Ad-hoc routing algorithms to which the technique is applied; 2) Type of wormhole detected: hidden or exposed or both; 3) Topology: dynamic or static; 4) Detection logic; 5) Requirements and/or key assumptions and 6) Wormhole prevention/detection capabilities.

The summary of the various wormhole prevention and detection techniques is presented in Table.2. Based on our review we present our analysis below.

In the wormhole detection techniques surveyed, routing protocols like, DSR AODV, DSDV and OLSR or a secure version of them is assumed to be the underlying protocol. It is observed from the table 2 that, techniques like [2] [17] [22]-[24] prevent both hidden and exposed wormholes. Wormhole is usually prevented or detected during the route establishment phase [13] [14] [28] and very few papers support detection of wormhole during data packet transmission [21].

Table.2. Summary of the various wormhole prevention and detection techniques

Prevention/Detection techniques	Technique applied to the routing algorithm	Wormhole detection type: hidden/ exposed/ both	Topology applicable	Detection logic based on	Requirements and/or key assumptions	Wormhole prevention/detection capability
LITEWORP 2005 [2]	On demand shortest path routing	Both	Static	Neighbor node monitoring	Special guard nodes and pre-distribution of keys to the nodes	Able to detect wormholes with 100% probability for 11 to 19 number of neighbors and reduces to 20 % for 20 to 37 numbers of neighbors
PW 2011 [3]	Wireless routing	Both	Cluster	Group membership	Advance encryption standard for group key and elliptic curve cryptography for secret key to secure the routing path	Would prevent the wormholes in large scale network because the cryptographic methods used are strong

SRAC 2009 [4]	DSR or AODV	Exposed	Dynamic	Neighbor node monitoring	Network must have disjoint paths to detect the wormhole	Able to detect malicious nodes up to 60% of total nodes
Packet leashes 2003 [13]	DSDV and Medium Access Control	Hidden	Static	Time and location	GPS and tight clock synchronization is required amongst all the nodes	Prevents the wormhole when packet leash condition is not satisfied
On mitigating in-band wormhole attack 2007 [14]	ARIADNE	Hidden	Dynamic	Time	Uses statistical profiling based on hop count	Detection rate at destination node is between 96% to 98% and at source node between 85% to 91%
Detecting and avoiding wormhole in OLSR 2007 [15]	OLSR	Hidden	Static	Time delay	End-to-end encryption between source and destination	95% wormhole detection rate for network of 30 node
SND scheme for 60 GHz directional network 2013 [16]	Proactive routing protocol	Hidden	Static	Time based	Centralized network with NC and directional antenna. Node authentication is based on El Gamal cryptography	Detection accuracy is 100% in a sector using NC broadcast and time analysis phase
WRSR 2013 [17]	Proactive and reactive protocol	Both	Static	Neighbor node monitoring	2-hop neighbor node list	For density of 4 to 7 wormholes, detection is between 94.67% to 100%
Label based secure localization scheme, 2015 [18]	Distance vector routing	Hidden	Dynamic	Neighbor node monitoring	DV-hop localization procedure to detect the wormhole link	Probability of a wormhole attack detection is above 95.4 % when the ratio of beacon node to sensor node is 30%
IVoW 2006 [19]	Wireless routing	Hidden	Dynamic	Connectivity Information	Multi-dimensional scaling and visualization of network topology	Detection accuracy varies from 100% to 97% when a wormhole varies from 1 to 5 in 500 node network
Time-based detection of wormhole, 2011 [20]	AODV	Hidden	Dynamic	Time delay based	Assumes that transmission delay through wormhole link is greater than normal link	Prevents wormhole attacks satisfactorily when traffic load is moderate (around 550 - 600Kbps)
ODSBR 2009 [21]	Secure SODV	Exposed	Dynamic	Delay and neighbor node monitoring	Source and destination nodes are trusted. Uses both symmetric and asymmetric key cryptography	Capable of delivering up-to 80% of the traffic when 5 wormholes are placed randomly, in a network of 50 nodes
DelPHI, 2006 [22]	AODV	Both	Dynamic	Time delay based	Needs multiple disjoint path to detect the wormhole	DelPHI can achieve more than 85% detection rate when tunnel length is greater than 4 hops
WAP, 2008, [23]	DSR	Both	Dynamic	Neighbor node monitoring	Assumes that packet delay through wormhole is always greater than wormhole free path	Throughput is increased by 14.2% when the WAP is applied on DSR protocol with node mobility of 10 m/s
Statistical wormhole detection, 2014, [24]	Hop-by-hop routing	both	Dynamic	Statistical neighbor count based	Computes average maximum hop-count using infrastructure nodes	Wormhole detection rate is 1.0 and false positives also 10% lesser as compared to other technique

4.1 ANALYSIS

From Table.2, in some cases, it is observed that the special hardware such as GPS, guard nodes or tight clock synchronization is required to accurately detect and locate the wormhole. However, in a low-cost MANET the GPS module will substantially increase the cost of the sensor node. Even, the number of guard nodes [2] or infrastructure nodes [24] required is proportional to the network area coverage. So the cost associated with the guard nodes or infrastructure nodes is also higher. Further, application of cryptography and hash algorithms to the routing packets add overheads in terms of time required to process and forward the packet. For example, in [4], CPU of 2.8GHz, RSA with 1024-bit key cryptographic operation requires 16.38ms and 1.7408 microseconds for one MD5 hash function. Similarly in [19], using 206MHz CPU, RSA encryption/decryption requires 56.70ms and 22.34ms for key size 512 and 1024 respectively. The exact cryptographic overheads of various cryptographic algorithm and energy consumption at each node are investigated in [30] and [31] respectively.

5. CONCLUSION AND FUTURE WORK

In this paper, we surveyed various hidden and exposed wormhole prevention and detection techniques for MANET. Security in ad-hoc routing process is required for ensuring privacy, integrity and availability. Secure routing protocols such as ARAN, ARIADNE, SAODV and SOLSR are vulnerable to wormhole attacks. Wormhole prevention techniques use cryptographic mechanisms; whereas, wormhole detection techniques use time delay and packet forwarding behavior for detection of the wormhole. However, the wormhole prevention techniques would tend to fail when the nodes are compromised well before the key distribution. Time delay based mechanisms would fail when the wormhole takes lesser time or has delay close to that of the wormhole free path. Neighbor node monitoring based mechanism need extra guard nodes or assume dense network setup, otherwise detection would be difficult.

Based on our review further investigation is required for the following: i) Detection of wormhole during data transmission is important as some wormholes with changing behavior may not be detected during route discovery and the wormhole could behave maliciously later. A mechanism like monitoring of packet delivery ratio could be used to detect such wormholes. ii) Detection of large number of wormhole tunnels and preventing them from appearing on subsequent routes. Monitoring of packet forwarding behavior by all the nodes in the MANET could be the solution for the identification of multiple tunnels, and iii) Prevention and detection of wormhole nodes even if they are using IP spoofing. Monitoring of packet forwarding behavior along with security mechanism like in [17] could be used to detect such wormholes.

REFERENCES

[1] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, “A Survey of Secure Mobile Ad-hoc Routing Protocols,” *IEEE Communications Surveys and Tutorials*, Vol. 10, No. 4, pp. 78-93, 2008.

[2] I. Khalil, S. Bagchi and N.B. Shroff, “Liteworp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, *Proceedings of International Conference on Dependable Systems and Networks*, pp. 612-621, 2005.

[3] Hao-Ting Pai and Fan Wu, “Prevention of Wormhole Attacks in Mobile Commerce Based on Non-infrastructure Wireless Networks,” *Electronic Commerce Research and Applications*, Vol. 10, No. 4, pp. 384-397, 2011.

[4] Ming Yu, Mengchu Zhou, and Wei Su, “A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments”, *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 1, pp. 449-460, 2009.

[5] Elizabeth M Royer and Chai-Keong Toh, “A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks”, *IEEE Personal Communications*, Vol. 6, No. 2, pp. 46-55, 1999.

[6] K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields and Elizabeth M. Belding-Royer, “Authenticated Routing for Ad Hoc Networks”, *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 3, pp. 598-610, 2005

[7] Yih Chun Hu, Adrian Perrig and David B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks”, *Wireless Networks*, Vol. 11, No. 1-2, pp. 21-38, 2005.

[8] Zhiguo Wan, Kui Ren and Ming Gu, “Usor: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks”, *IEEE Transactions on Wireless Communications*, Vol. 11, No. 5, pp. 1922-1932, 2012.

[9] M.G. Zapata and N. Asokan, “Securing Ad hoc Routing Protocols”, *Proceedings of 1st ACM Workshop on Wireless Security*, pp. 1-10, 2002.

[10] Fan Hong, Cai. Fu and Liang Hong, “Secure OLSR”, *Proceedings of 19th International Conference on Advanced Information Networking and Applications*, pp. 1-6, 2005.

[11] Yin Chun Hu, David.B. Johnson and Adrian Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, *Ad Hoc Networks*, Vol. 1, No. 1, pp. 175-192, 2003.

[12] P. Papadimitratos and Z.J. Haas, “Securing the Internet Routing Infrastructure,” *IEEE Communications Magazine*, Vol. 40, No. 10, pp. 60-68, 2002.

[13] Yin Chun Hu, David B. Johnson and Adrian Perrig, “Wormhole Attacks in Wireless Networks”, *IEEE Journal on Selected Areas in Communications,* Vol. 24, No. 2, pp. 370-380, 2006.

[14] Xu Su and R.V. Boppana, “On Mitigating In-band Wormhole Attacks in Mobile Ad-hoc Networks”, *Proceedings of IEEE International Conference on Communications*, pp. 1136-1141, 2007.

[15] F. Nait-Abdesselam, B. Bensaou and T. Taleb, “Detecting and Avoiding Wormhole Attacks in Wireless Ad-hoc Networks”, *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 127-133, 2008.

[16] Zhiguo Shi, Ruixue Sun, Rongxing Lu, Jian Qiao, Jiming Chen and Xuemin Shen, “A Wormhole Attack Resistant Neighbor Discovery Scheme With RDMA Protocol for 60 GHz Directional Network,” *IEEE Transactions on Emerging Topics in Computing,* Vol. 1, No. 2, pp. 341-352, 2013.

[17] Rakesh Matam and Somanath Tripathy, "WRSR: Wormhole-Resilient Secure Routing for Wireless Mesh Networks", *EURASIP Journal on Wireless Communications and Networking*, pp. 1-12, 2013

[18] Honglong Chen et al., "Securing DV-Hop localization against Wormhole Attacks in Wireless Sensor Networks", *Pervasive and Mobile Computing*, Vol. 16, pp. 22-35, 2015.

[19] Weichao Wang and Aidong Lu, "Interactive Wormhole Detection in Large Scale Wireless Network", *Proceedings of IEEE Symposium on Visual Analytics Science and Technology*, pp. 99-106, 2006.

[20] Fei Shi, Dongxu Jin, Weijie Liu and Joo Seok Song, "Time-based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks", *Proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1721-1726, 2011.

[21] Baurch Awerbuch *et al.*, "Odsbr: An On-demand Secure Byzantine Resilient Routing Protocol for Wireless Ad-hoc Networks", *ACM Transactions on Information System Security*, Vol. 10, No. 4, pp. 1-35, 2008.

[22] Hon Sun Chiu and King Shan Lui, "Delphi: Wormhole Detection Mechanism for Ad Hoc Wireless Network", *Proceedings of International Symposium on Wireless Pervasive Computing*, pp. 1-6, 2006.

[23] Sun Choi, Doo-young Kim, Do-hyeon Lee and Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 343-348, 2008.

[24] Thi Ngoc Diep Pham and Chai Kiat Yeo. "Statistical Wormhole Detection and Localization in Delay Tolerant Networks", *Proceedings of* IEEE *Conference on 11th Consumer Communications and Networking*, pp. 380-385, 2014.

[25] Yue Cao and Zhili Sun, "Routing in Delay/disruption Tolerant Networks: A Taxonomy, Survey and Challenges", *IEEE Communications Surveys and Tutorials*, Vol. 15, No. 2, pp. 654-677, 2013.

[26] R. Maheshwari, J. Gao and S.R. Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information", *Proceedings of IEEE 26th IEEE International Conference on Computer Communications*, pp. 107-115, 2007

[27] Rupinder Singh, Jatinder Singh and Ravinder Singh, "Wrht: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks", *Mobile Information Systems*, Vol. 2016, pp. 1-13, 2016

[28] Lishi Chen, Chunyan Liu and Hejiao Huang, "Secure Routing against Wormhole Attack and its Formal Verification based on Timed Colored Petri Net", *Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pp. 157-164, 2015.

[29] Honglong Chen, Wei Lou, and Zhi Wang, "On Providing Wormhole Attack Resistant Localization using Conflicting Sets", *Wireless Communications and Mobile Computing*, Vol. 15, No. 15, pp. 1865-1881, 2015.

[30] P. Ganesan et al., "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", *Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications*, pp. 151-159, 2003.

[31] N.R. Potlapally et al., "Analyzing the Energy Consumption of Security Protocols", *Proceedings of International Symposium on Low Power Electronics and* Design, pp 30-35, 2003.