An analytical survey of state of the art wormhole detection and prevention techniques

Zubair Ahmed Khan, Saeed Ur Rehman, M Hasan Islam
Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan
Email: Zubair530@gmail.com, saeed@case.edu.pk, mhasanislam@gmail.com

Abstract—Due to the current enhancements in the wireless technologies Mobile Ad hoc Networks (MANETs) are becoming more and more common. Previously little effort was given towards the security in MANETs, but now due to increase in use of MANETs serious attention is required towards the security of MANETs. A number of different attacks have been discovered that can be launched against MANETs. Wormhole attack is one such attack that has been recently discovered. Wormhole attack is a very severe and challenging attack because of the fact that it can be launched against any protocol and also due to its ability to be effective in case of encrypted traffic. Enormous amount of work has been done towards the mitigation of wormhole attack and its counter measure. In this paper we have tried to combine all the previous research done against the wormhole attack and to summarize the efforts previously done, our aim here is to provide the researchers a platform where they can find a complete reference to all past work done in regards to the wormhole attack. A comparative analysis of the techniques reveals that there is not a single solution available that can comprehensively handle the wormhole attack. In the end we have identified the goals for an ideal solution for the wormhole attack.

Index Terms— Wormhole attack, Mobile Ad hoc Network, MANET, Security, Survey, Limitations

1 INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a recent enhancement in the technologies which relieves us from the expensive deployment costs. It is a self-configurable infrastructure less network of mobile devices. These networks provide closer interaction with humans as compared to the other types of Ad hoc Networks. Here Nodes are multipurpose and can perform more than one function at a time.
It can be built in areas where there is no existing infrastructure or it has been destroyed due some disastrous situations (e.g. War, Earthquakes or Tsunamis etc…). In fact; For a MANET there is no need to build an infrastructure because it is a collection of mobile nodes which create a network with one another on ad-hoc basis and are mostly used in situations where a temporary solution is required. MANETs are more vulnerable to attacks as compared to wired network because of their boundless medium, dynamic topology and weak nodes (processing power and battery life).

2 SECURITY IN MANETS:

Security of MANETs is an area that has been overlooked because of the assumptions that all nodes are honest and also because of scarce resources available to mobile nodes. The lack of security measures in the Ad hoc routing protocols has lured enormous number of intruders into attacking the ad hoc networks. This is also due to deployment of MANETs into a number of different application requirements. Security requirements can change drastically from application to application which also makes security implementation very much difficult. For example security requirements in a battle communication as compared to security requirement in a Wi-Fi/internet hotspot location.
There can be a number of different types of attacks launched against a network. There are attacks in which more than one attacker combine/synchronize their actions to launch some attack on a network. E.g. Black hole attack, Sybil attack, wormhole attack. There are some attacks which cannot be put under one classification category and whose effects are scattered across many dimensions. These attacks can be a foundation point for other severe attacks and also can launch a number of different attacks. An example of such an attack is a "Wormhole Attack".

2.1 Wormhole Attack:

In a wormhole attack [1] two nodes are connected with one another with the help of a medium which is not available to normal nodes, with the help of this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot. The two colluding nodes act in a way that they appear to be neighbors to all the other nodes.

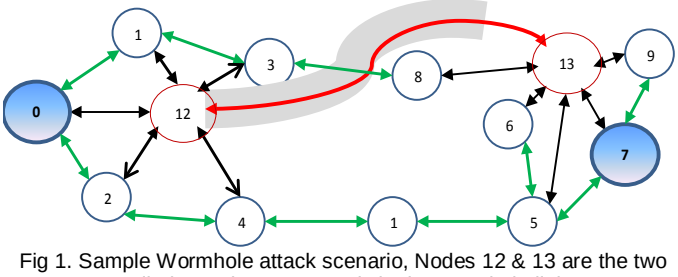

Fig 1. Sample Wormhole attack scenario, Nodes 12 & 13 are the two colluder nodes connected via the wormhole link

Looking at Fig. 1, suppose node-0 wants path to node-7 along

the network, node-0 broadcasts a route request. Suppose node-12 and node-13 are the two colluder nodes in the vicinity of source and destination nodes; respectively. Node-12 along with other nodes near the source receives the route request, it replays the same request to node-13 through it's out of band channel, node-13 receives the packet de-capsulate it and rebroadcasts it in its neighborhood. Upon receiving the route request (via node-13) the nodes at the destination (e.g. nodes - 6, 7, and 9) will feel that they are direct neighbors to node-0, and will reply to the route request. Node-13 will capture the reply and using the same procedure will send it to node-12; which will send it to node-0. Thus node-0 and node-7 will assume that they are one hop neighbors. And whole of their communication will have to pass through node-12 and node-13. This is one type of wormhole attack (Hidden wormhole attack); there are a number of variants defined in the literature [9], [5], [10].

The wormhole attack is a very powerful and severe attack in the sense that it does not need to break the cryptographic measures in order to be successful. E.g. they can simply capture and encapsulate all the traffic received and tunnel it to other end of wormhole, where it is de capsulated and replayed there. It can be launched against all types of protocols, reactive and proactive protocols are all vulnerable to the wormhole attack [11], [8]. The attackers can remain invisible and still be able to launch the wormhole attack (hidden wormhole attack). And there are a number of variations of wormhole present that give them the ability to deceive almost all solutions proposed in the literature.

A wormhole attack is a Collaborative Attack [2], [3] because there are more than one attackers involved. It is a Network Layer Attack [4] because it occurs at the network layer and disrupts routing information. It can be launched using Fabrication technique [5], [6]. It can also be launched using Replay [7], [8]. It is independent of routing Protocols because it can be launched against all types routing protocols. It is also independent of cryptographic measures because the attackers don't need to decrypt the network traffic in order to launch the attack.

The wormhole attackers seems to provide quite a useful service in terms of providing the shortest path to other nodes; but as it seems to be, it is not always the case and makes the integrity of the whole network at stake.

2.1.1 Threats due to Wormhole attack:

Wormhole is a serious Threat to the network and has the ability to cause:

1. Alterations in network and Base Station Deceptions [9]
2. Results in routing information corruption [8]
3. Can cause failure of Localization Dependent protocols. E.g. target tracking applications, Can corrupt data delivery
4. Can be launched upon any of the current routing protocols [11], e.g. DSR, AODV, DSDV, OLSR etc…
5. Can penetrate wrong route/topology information into the network [12], Thereby, defeating the purpose of routing algorithms.
6. The type of attack that allows the attackers to launch a number of other attacks also, e.g. black hole, grey hole, DOS, sinkhole

2.1.2 Effects of Wormhole Attack:

Results of wormhole success can be very devastating. There are a lot of effects mentioned in the literature that can happen due to wormhole presence in the network:

1. Allows the attacker to
   1.1. Gain unauthorized access,
   1.2. Disrupt routing
   1.3. Launch denial-of-service attacks (DoS)
   1.4. Launch the black hole attacks (by dropping all data packets)
   1.5. Grey hole attacks (by selectively dropping data packets)
   1.6. Launch cryptanalysis Attacks
   1.7. Crack communication keys
   1.8. Degrades services at physical layer
   1.9. Surveillance/Alarm system corruption
2. At the end legitimate paths cannot be found
3. Some nodes might get isolated from whole network and will not be able to communicate at all.

2.1.3 Symptoms/ Results of Wormhole Attack:

Once a successful wormhole attack is launched there are certain symptoms that can be observed in the network, following are some of the symptoms mentioned in the literature.

1. Abrupt decreases in hops
2. Abrupt increase in path delays
3. Longer propagation delays
4. Decrease in network utilization
5. One link getting higher usage ratio than others
6. Reception of data from a far apart node
7. Reception of multiple copies of same message
8. Reception of one's own messages back

2.2 Summary

A wormhole attack is a very serious threat to the security triad (Confidentiality, Integrity and Availability) of the Mobile Ad-hoc Network and it must be treated as a highest priority threat [40], [42], [44], [46], [47]. In the following section we are presenting a comprehensive literature survey of the wormhole attack mitigation techniques presented in the literature. As the literature survey reveals, the enormous amount of research being done in this direction proves our claim about its importance.

3 Literature Survey:

Since the introduction of wormhole attack concept in 2003 by Hu et al. [1] tremendous amount of research has been done in this direction. Different researchers have tried to handle the attack differently. These proposed techniques ranges from the use of extra and expensive hardware to use of highly

synchronized clocks and from addition of new fields in the packets to the introduction of additional fields in the routing protocols.

3.1 Classification of Techniques:

We can broadly classify those techniques into the following different types:

3.1.1 **Hardware Based**: These techniques require the use of extra hardware for the use of for the detection of wormhole attacks. The hardware required can be GPS hardware or some specialized hardware for detection/avoidance of wormhole attacks. Some techniques also propose the use of specialized nodes. These techniques due to the requirement of extra hardware are either very expensive or processing intensive not viable for the concept of MANETs. Examples of this technique are [1],[13], [14], [15], [16], [11], [17], [18], [12], [19], [20], [21], [3] and [22]

3.1.2 **Clock Based**: These techniques the nodes to have tightly synchronized clocks so that they are able to detect any anomalies in the network. To achieve clock synchronization in the highly dynamic nature of MANET itself seems a tough ask to do. Examples of these include [1], [5], [11], [13], [17], [18], [21], [23], [24], [25], [26] and [27].

3.1.3 **Packet Leashes Based**: These techniques limits the journey of packets across the network beyond a certain limit (either distance or time). They in turn require either GPS hardware or tightly synchronized clocks. These techniques introduce some information in the packet headers; every node along the path is supposed to check that information and is supposed to drop the packets if the packet has travelled beyond its limits. These techniques are good only for avoidance of wormhole attacks. Examples of this technique are [1], [5], [13] and [28]

3.1.4 **RTT Based**: These techniques use the Round Trip time for the detection of wormhole attacks present along a path. Use RTT alone is insufficient; since attackers might be able to use high speed links to make their delays undetected or use store and forward type of wormhole attack. Examples of this techniques are [29], [30], [31] and [26]

3.1.5 **TTL Based**: These techniques are similar to the Packet Leashes based approaches, since they monitor the Time-To-Live field in the packet to identify suspicious paths. Again; here we will require tightly synchronized clocks. Examples of this is [5]

3.1.6 **Neighbor Discovery/Verification Based**: These techniques uses neighbor/network information for the detection of wormhole attacks. This may either involve verification from neighbors, neighbor information or neighbor monitoring to detect the wormhole attack. Examples of this are [4], [5], [6], [11], [16], [21], [24], [25], [32], [33], [34], [35] and [36]

3.1.7 **Others**: There are a number of other techniques present in the literature that try to avoid/detect or mitigate the wormhole attacks according to their own perception of the attack. E.g. Graphical Techniques [8] and [37], Statistical Techniques [48] and a number of others [12], [17], [19], [20], [38], and [39]

3.2 Existing Solutions:

In our previous work [36] we have utilized the built-in routing table and neighbors' verification for the detection of exposed wormhole attack.

This section contains the summary of different techniques present in the literature for the detection of wormhole attacks. These techniques are listed according to the year of publication, with most recent ones first.

In 2012, S. K. Dhurandher et al. [3] proposed E2SIW (Energy-Efficient Scheme Immune to Wormhole attacks) for the prevention of wormhole attacks, they use location information received from the GPS hardware. The approach only tries to prevent the wormhole attack; it doesn't take into consideration the detection of the wormhole nodes and their punishment. The approach is also limited by the requirement of GPS Hardware.

In 2012, A. Malhotra et al. [12] proposed a clustering and digital signature based approach for avoidance and prevention of wormhole attacks. The algorithm needs some nodes to perform specialized functions also, e.g. some nodes are supposed to be Cluster Heads and some are assumed to be Gateway nodes. The model built assumes transmission through on Cluster heads and Gateway nodes and dropping traffic arising from any other model. The algorithm seems good only for avoidance of wormhole link, it cannot identify the attackers nor perform any mitigation any of the identified nodes.

In 2012, Shalabh Jain et al. [38] proposed a scheme based upon the wireless channel properties for the detection of wormhole attack. They used the electromagnetic wave propagation and Channel State information for detection of wormhole in the network. The base of their algorithm is the alterations in symmetry of Channel State Information due to presence of wormhole adversaries. They look for changes in symmetries at both ends of the wormhole. The approach also doesn't provide pinpointing of attackers and hence doesn't account for the accountability of the attackers. The approach also seems to be computationally intensive and will need extra processing.

In 2012, Soo-Young Shin et al. [30] proposed a three step based wormhole detection scheme, the scheme detects the delayed response (RTT) from wormhole path as compared to normal paths received during path discovery step. Being based upon delayed RTT, the approach can only detect the tunneling/encapsulation variant of the wormhole. If the attackers are connected using a high speed high transmission link, the algorithm is most likely to fail. In normal scenario a routing protocol will accept only the first route reply and will

drop any further requests, the algorithm also requires storing all the replies and then performing a comparison among them.

In 2012, S. Hazra et al. [19] proposed "CAT-AODV-W" (Context Aware Trusted AODV against Wormhole attack). A trust based mechanism for making decision of whether to communicate or not communicate with another node. The trust of a node is built upon its previous communication history. Due to the dynamic nature of MANETs the concept does not seem much promising. The technique also is only proposed for AODV and other protocols have not been taken into account. The mechanism seems to be an avoidance mechanism rather than a detection and mitigation mechanism.

In 2012, S. Song et al. [33] proposed SWAN (Statistical Wormhole Apprehension using Neighbors). The algorithm proposes the use of neighbor discovery in another way for the detection of wormhole attack. SWAN uses the increase in number of neighbors detected in a region where wormhole exists. Authors assume that the number of neighbors will increase in regions of wormhole. Though the existence of wormhole detection is proposed there is no reference as how to pinpoint the attackers or to handle the wormhole attack.

In 2012, T. Zhang et al. [20] proposed SDVL (secure DV-Hop localization scheme). SDVL works by monitoring neighbor nodes behavior in a network and decides whether a wormhole is present or not. Exposed wormhole is detected by the neighbors' behavior whereas hidden node is inferred from the discrepancies in the hop size received by the beacons. Nodes need to calculate their position with respect to beacon nodes which already know their position. The approach is proposed for Wireless Sensor Networks and hence doesn't take mobility into account.

In 2012, R. Jaiswal et al. [39] proposed RBS (Reference broadcast Synchronization) which uses of entropy of a node in a multicast group for detection of abnormal/wormhole nodes. The approach seems promising but is not very well explained. It might also not be able to detect a hidden wormhole.

In 2012, S. Jain et al. [34] proposed the use of secure neighbor discovery for the mitigation of wormhole attacks. They look for apparent channel noise due to replay and encapsulation performed by wormhole nodes. The approach seems be only taking the exposed wormhole into account.

In 2012, T. Divya et al. [21] proposed the use of honeypots for locating the wormhole attackers. Honeypots are used to identify attackers and their usual behavior after the attack is launched. They identify the attackers by neighbor monitoring. Neighbors are monitored by keeping history of their RREQ communication and identifying whether they replied selflessly or not. The approach is limited by neighbor monitoring and GPS requirements. They also use Packet Travel Time (PTT) which will need a strongly synchronized clock.

In 2012, S. Upadhyay et al. [35] proposed a statistical analysis approach for avoidance of wormhole attacks. The proposed algorithm is based upon the statistics of incoming/outgoing packets and the average delay incurred during a path setup. The algorithm works by finding routes in reactive fashion for paths already found and then averaging the time consumed by finding each path, the paths which have taken longest/smallest time are blacklisted. The approach is expensive in terms of processing also doesn't takes the false alarms into account that will be generated by black listing normal paths.

In 2012, V. Karthik Raju et al. [31] proposed the use of Average One hop RTT to calculate average time of larger paths to avoid wormhole links. If a link has taken more time than the Average RTT times hops of the link, it is considered as suspicious and is not used for further communications. The approach is likely to fail when the attackers are connected via a high speed link or there is congestion in network hence generating false alarms. Clearly; we need something more than just Average RTT to successfully identify wormhole links.

In 2012, Ali Modirkhazeni et al. [41] proposed the use of Neighbor discovery for avoidance of wormhole links. The algorithm assumes that nodes knows their neighbors and hence will not receive any data that is received from one of its non-neighbor nodes. It is assumed that nodes will probe their neighbors during initial network setup phase and also wormhole is not possible during that stage. The approach being proposed for WSNs doesn't take mobility into account and doesn't allow for addition/removal of new nodes to/from the network.

In 2012, T. Sakthivel et al. [26] proposed PT (Path Tracing) Algorithm for the detection of wormhole attacks. PT calculates the distance travelled per hop by calculating it using RTT and Speed of light. The distance is used for identification of abnormal routes. A normal distance is stored in the routing table which will be used as a threshold value for newly created paths. Timestamps are added to packets before sending hence requiring clock synchronization. The per hop distance calculated by the source is also sent in the packet header. Each node in the path which receives the packet has to compare its calculated distance with the value that is present in the packet header. As a final check they test the number of appearances if the suspicious route in the routing table. The approach seems to be promising but it needs clock synchronization, takes only reactive protocol (DSR) into account and needs to calculate the distance. The clock synchronization and distance calculation seems to be a tough ask looking at the disconnected nature of the Adhoc Networks.

In 2012, K.G. Reddy et al. [27] proposed the use of end-to-end delay calculations for the detection of wormhole attacks in wireless mesh networks. The approach is limited by fact that we will need tight time synchronization to calculate the end to end delays. The technique is likely to fail if the attackers are connected through a high power and low latency link.

In 2012, Y. Zhang et al. [28] proposed SOLSR (Secure Optimistic Link State Routing Protocol). SOLSR is based upon the idea of location based broadcast keys. Every node has a different key for transmission through paths of different hops; i.e. one hop neighbors will receive data encrypted with one key and three hops neighbors will receive data encrypted with another key. The approach seems to work for avoidance of wormhole, but the overhead incurred due to sharing and generating the keyset is extraneous. The algorithm will face scalability issues to a very large extent because the number of keys required to be stored at a particular node will increase drastically due to increase in hops and number of nodes. There will be a lot of overhead incurred

due to nodes movement which is a characteristic of an ad hoc network.

In 2012, S. Vijayalakshmi et al. [22] proposed CTT (Cumulative Threshold Transmission Rate) for the use of wormhole detection in a MANET. CTT takes into account three characteristics of a network before and after a wormhole is launched. The Transmission Rate (Cumulative Transmission Rate), Route Cache Mismatch and hop count mismatch. This means that we have to keep history of these three measures. The detection is done by Key Master Agent and slave agents that are monitoring the other network nodes, meaning if a node that is not in the range of either Master or Slave agent can pass by un-detected. The approach is likely to fail in case of frequent node movements, since the route cache will be changing frequently. In case of addition of new nodes the approach will also fail, since we do not have their CTR already calculated.

In 2012, Oya Simsek et al. [45] proposed a distributed approach which takes into account a nodes' neighbor density and uses it for the detection of wormhole attacks. During an initial discovery phase a node must find its neighbors and has to calculate its own neighbor density and standard deviation. All the nodes share this information to identify nodes with abnormal node density and neighbors. The approach takes only exposed node into account and might not be able to detect hidden wormhole.

In 2011, Modirkhazeni et al. [43] proposed neighbor discovery technique for handling wormhole attack. They look for data from unauthorized nodes/neighbors. It is assumed that nodes are static and number of nodes is fixed and every node identifies its authorized neighbors in initial stage and later rejects data from all nodes which are not authorized neighbors. The technique is quite effective in cases where we have static and fixed number of nodes. But it is not flexible in case where one need mobility and has no scalability.

In 2011, S. Vijayalakshmi et al. [5] proposed an approach which uses time based leashes (Limiting Packet Propagation Parameter LP3) and Neighbor monitoring technique (NAWA2) for avoidance and detection of wormhole attacks. Though they don't need extra hardware but requires tightly synchronized clocks (for LP3), so as to apply fix timing constraints (TTL) on journey of packets across networks. TTL is a value which expires after some time which is calculated according to the network RTT. Suspicious nodes are detected by a collaborative approach by its neighbors (Neighbor Aware Wormhole Adversary Axing NAWA2). The neighbors look for Multicast Packet Delivery Ratio and Jitter for the node under suspicion. Using LP3 and NAWA2 we can only detect the encapsulation variant of wormhole attack, because other variants may not have significant delay/jitter on data. We also need to take care of the LP3 parameter by encrypting or digitally signing. NAWA2 seems to be ineffective in case where we don't have neighbors of the suspicious nodes.

In 2011, A. Vani et al. [4] proposed a hop count and neighbors' list comparison for the detection of wormhole attacks. They have proposed a new secure protocol for AODV called as WARDP, which selects link-disjoint multi-paths in the route-discovery procedure to avoid wormholes. Wormhole is detected by the hop count monitoring and neighbors' neighbor list comparison. The algorithm poses extra load on nodes in terms of memory, processing and network resources. It'll need extra copies of routes for history of hop counts. It'll also need extra memory, processing and network resources during neighbor list exchange. The algorithm also doesn't take into consideration the false alarms which can arise due to removal of all suspicious nodes.

In 2010, Chen et al. [18] proposed a conflicting set based secure location approach. The approach is based upon Received Signal Strength Indicator (RSSI) based distance estimation between nodes and locators. Locators are fixed nodes that know their location in advance. The approach is proposed for Static networks and mobility has not been taken into consideration. It also needs clock synchronization and distance estimation cannot be accurate.

In 2009, Venkataraman et al. [37] proposed a graph theoretic algorithm for the detection of wormhole attack. An adjacency matrix is built from the routing table of a node running a proactive protocol. Nodes are required to Square the matrix (i.e. Matrix multiplication) and then compare it to Squared Matrix of some other node. The results are compared to identify whether the nodes are neighbors are not. The approach seems to be computationally expensive due to the matrix involvement.

In 2009, Shokri et al. [17] proposed a secure neighbor discovery protocol that depends upon a cooperative approach among the neighbors. The algorithm requires Ultrasound (US) and Radio Frequency (RF) based ranging protocol for distance estimation among nodes. The algorithm is supposed for Constrained Static WSNs. Each node is supposed to be equipped with two interfaces an US and RF Interface.

In 2008, I Khalil et al. [32] proposed MOBIWORP. MOBIWORP is a neighbor monitoring based protocol in which nodes monitor the activities performed by their neighbors. Local monitoring is done by guard nodes. There is a Central authority which is responsible for global monitoring and converges feedback provided by the guard nodes. CA is also responsible for handshake and key exchange with mobile nodes. Each mobile node has a key shared with the CA. Every node keeps a list of its two hop neighbors. MOBIWORP is highly dependent upon neighbor communication and requires extra processing.

In 2008, Papadimitratos et al. [24], [25] proposed Secure Neighbor discovery approach. It is based upon the assumptions that a node can avoid wormhole if it is able to correctly identify its neighbors. Two nodes verify one another by the use of feasible traces. It is assumed that clocks are synchronized and nodes are static.

In 2007, Tran et al. [29] proposed TTM (Transmission Time based Mechanism). TTM is a collaborative approach among neighbor nodes along a path. During the Route Setup procedure RTT is calculated between each neighbor and is sent along with the path to the source node. The source node can then check all the RTTs and can identify a link (among two nodes) that has a higher RTT. TTM seems good for situations of hidden wormhole. However the RTT can also increase due to some

other factors e.g. congestion. The approach also seems un-sufficient in cases where an exposed wormhole exists and attackers are connected via a high transmission link. Also if the approach is based upon Transmission Time between two successive nodes, we will need synchronized clocks. If it is RTT based this will mean extra overhead during path setup.

In 2007, Maheshwari et al. [8] proposed a connectivity graph based approach. The algorithm takes into account the local connectivity based information to build graphs. These graphs are called Unit Disc Graphs (UDG) with the node at its center. An invalid UDG will mean a wormhole existence. A UDG is invalid if it contains forbidden substructures e.g. too many nodes in UDG without having edges in between them. The algorithm seems good for hidden wormhole; it will not be able to detect the exposed wormhole, because one end will appear in one UDG and other in another.

In 2006, Chiu et al. [23] proposed DELPHI, Delay Per Hop Indication. They observe delay per hop from source to destination for different paths for wormhole detection. The approach is likely to detect only the encapsulation form of the wormhole attack. Other types (e.g. Out of Band or High transmission) of wormholes might use highly sophisticated hardware to reduce the delays. The approach only handles the detection of wormhole attack and cannot pin point the exact location of the wormhole nodes.

In 2006, Eriksson et al. [11] proposed TrueLink, which is a MAC Layer extension to the standard IEEE 802.11 MAC layer. It is timing and authentication based technique. Nodes have the capability to detect the existence of direct link between its neighbors. The link is verified using a two-step procedure which needs very tight timing constraints in order to be able to correctly identify a valid link. TrueLink also requires a backwards compatible firmware update to the standard IEEE 802.11 hardware. We will also need to have very tight timing measurements for the nonce phase.

In 2005, Song et al. [48] proposed a Statistical Analysis based approach (SAM). SAM monitors the occurrence of links returned for a particular destination in multipath protocols. SAM is based upon the theory that since wormhole links offer the shortest path from a particular source to destination, they will be found in higher percentage than other links. SAM being applied on Multipath protocols and only for a single pair of source/destination might not be very effective.

In 2005, Khalil et al. [6] proposed LITEWORP, which relies upon overhearing neighbor communications. Each node is assumed to keep list of its one and two hop neighbors, the discovery is done just once in the lifetime of nodes. The main theme is not to accept any data from a node that is not present in any of the two lists. Every node is supposed to monitor its neighbors' traffic by keeping a time stamped copy of every packet sent/received by its neighbors. Though the technique seems to avoid the wormhole attack, it is limited by assumptions of a static topology and no new nodes being able to connect to the network.

In 2004, Weng et al. [14] proposed MDS-VOW (Multidimensional Scaling). MDS builds the layout of the sensors' network and then performs wormhole detection by looking for anomalies in the constructed graph. The absence of wormhole is inferred from smoothness of the constructed layout, if any wormhole exists in the network the layout will not be smooth; instead there will be bending at the point of wormhole. Although the approach seems very interesting, we will need correct distance between nodes and their locations (e.g. GPS Coordinates) and it is proposed for Sensor Network where mobility is not taken into account.

In 2004, Lazos et al. [15] proposed SerLoc. SerLoc is a Security-aware range-independent localization scheme for WSN. The proposed the use of Omni-directional antenna on every sensor node. Sensors are dependent for their location on specialized nodes called locators. Locators know their location in advance and broadcasts beacons periodically. Each sensor after receiving beacon can find its location. A beacon comprises of locators coordinates and the corresponding antenna sector. The approach is proposed for WSNs only, hence the mobility is not taken into account and it will not be possible to install Omni-directional antenna on every sensor.

In 2004, Hu et al. [16] proposed the use of Directional antennas for handling of wormhole attacks. Their main motive is to avoid nodes that give incorrect location information by installing directional antennas. By keeping list of its one hop neighbors a node can avoid wormhole node by rejecting any traffic from any non-neighbor node. It is wormhole avoidance, rather than a detection or prevention scheme. The requirement of Directional Antenna and Line of sight requirement makes it difficult to practically implement. Again it is a WSN based technique where Mobility is not taken into consideration.A node after once discovering its neighbors will not be able to find new neighbors.

In 2003, Hu et al. [1] introduced the concept of wormhole and also its countermeasures. They introduced the concept of Leashes for prevention of wormholes. Both geographical (limit travelled distance) and temporal (limiting travelling time) leashes were proposed to avoid the wormhole attack. A new protocol TIK (TESLA with Instant Key disclosure) was introduced to handle the temporal leashes. The approach seemingly limited by GPS Hardware requirement (Geographical Leashes) and tight clock synchronization (Temporal Leashes) issues, is a good way to avoid the wormhole attack. Although it doesn't detect the existence of wormhole and identifying the culprit nodes, it is a good approach for avoidance of wormhole attack.

In 2003, Capkun et al. [13] proposed SECTOR, which assumes nodes with extra hardware for fast one bit extra processing and nodes with nanoseconds time accuracy. Proposed a distance bounding based protocol MAD (Mutual authenticated Distance Bounding), which is an authenticated protocol. MAD is used for finding distance between to neighbors. It may not need location information or tight time synchronization, it needs specialized hardware and efficient MAC handling for processing the challenge with minimal delay.

TABLE 1: COMPARISON OF EXISTING WORMHOLE TECHNIQUES WITH RESPECT TO THE REQUIREMENTS.

Technique	Leash	Attack Type	H/W	Time Sync	Special Nodes
CSI & RSSI [38]	No	Hidden	No	No	No
RTT per Hop [30]	No	Exposed	No	No	No
CAT-AODV-W[19]	No	Exposed	No	No	Yes
SDVL[20]	No	Both	No	No	Yes
Secure Neighbor Discovery[34]	No	Exposed	No	No	No
Honeypots [21]	No	Exposed	GPS	Yes	No
Statistical Analysis [35]	No		No	No	No
RTT Estimation[31]	No	Hidden	No	No	No
Network Discovery[41]	No	Hidden	No	No	No
E2SIW[3]	No	Both	GPS	No	No
Path Tracing[26]	No	Exposed	No	Yes	No
Delay based[27]	No		No	Yes	No
SOLSR[28]	LBKs	Hidden	No	No	No
CTT [22]	No	Hidden	No	No	Yes
Network Discovery[45]	No	Exposed	No	No	No
Routing Table [36]	No	Exposed	No	No	No
Neighbor discovery [43]	No	Hidden	No	No	No
WARDP[4]	No	Exposed	No	No	No
Secure Localization [18]	No	Hidden	No	Yes	Yes
graph theoretic Approach [37]	No		No	No	No
US + RF [17]	No	Exposed	Yes	Yes	Yes
MOBIWORP [32]	No	Exposed	No	No	Yes
Secure Neighbor Discovery [25]	No	Hidden	No	Yes	No
TTM[29]	No	Hidden	No	No	No
Connectivity Graph[8]	No	Hidden	No	No	No
DELPHI[23]		Exposed	No	Yes	No
SAM[48]	No	Exposed	No	No	No
LITEWORP[6]	No	Both	No	No	Yes
Directional Antennas [16]	No	Hidden	Yes	No	No
Packet Leashes[1]	Yes	Both	Yes	Yes	No

TABLE 2: COMPARISON OF WORMHOLE TECHNIQUES WITH RESPECT TO THE DETECTION CAPABILITIES AND TARGET NETWORK.

Technique	Network	Mobility	Prevention	Detection	Removal
Clustering and Digital Signatures [12]	MANETs	Yes	Yes	No	No
CSI & RSSI [38]	MANETs	Yes	Yes	No	no
RTT per Hop [30]	MANETs	Yes	No	Yes	No
CAT-AODV-W [19]	MANETs	Yes	Yes	No	No
SWAN [33]	mWSN	Yes			
SDVL [20]	WSN	No	No	Yes	No
RBS [39]	MANETs	Yes	No	Yes	No
Secure Neighbor Discovery [34]	MANETs	Yes	No	Yes	No
Honeypots [21]	MANETs	Yes	No	Yes	Yes
Statistical Analysis [35]	MANETs	Yes	Yes	No	No
RTT Estimation [31]	MANETs	Yes	Yes	Yes	No
Network Discovery [41]	WSN	No	Yes	Yes	No
E2SIW [3]	N/A		Yes	No	No
Path Tracing [26]	MANETs	Yes	Yes	Yes	Yes
Delay based [27]	WMN	Yes	No	Yes	No
SOLSR [28]	N/A		Yes	No	No
CTT [22]	MANETs	Yes	No	Yes	Yes
Network Discovery [45]	WSN	Yes	No	Yes	Yes
Routing Table [36]	MANETs	Yes	Yes	Yes	Yes
neighbor discovery [43]	WSN	No	Yes	Yes	
Distance estimation [18]	WSN	No	No	Yes	Yes
US + RF [17]	WSN	No	No	Yes	No
Secure Neighbor Discovery - neighbor discovery [25]	WSN	No	Yes	No	No
LITEWORP [6]	WSN	No	Yes	Yes	No
MDS - VOW [14]	WSN	No	Yes	Yes	
SERLOC [15]	WSN	No	Yes	No	No
Directional Antennas [16]	WSN	No	Yes	No	No
Packet Leashes [1]	N/A		Yes	No	No
SECTOR [13]	WSN		Yes	Yes	

4 CONCLUSION

Literature review reveals that none of the solutions proposed in the literature is perfect. In fact every solution takes only one dimension of the wormhole attack detection process [Table 1 & 2] for example if one solution doesn't need extra hardware it may require tight time synchronization which is itself a tough ask. On the other hand if a solution doesn't need extra hardware and time synchronization both, it cannot detect both types of wormhole attacks (Hidden + exposed).

If a solution is able to detect both types of attacks, it might have either overlooked mobility or has taken detection of wormhole into account. What we require is; a solution that can handle each and every aspect mentioned in literature and in the table. Hence we can say that major points of an ideal wormhole solution can be stated as.

1. **Minimal change** to existing implementations
   - Use already available information
   - Minimize use of extra information
2. **Protocol Independence**: A solution that can detect wormhole independent of the protocol type.
3. **No extra hardware**: A solution will not require any extra hardware
4. **No time synchronization**: A solution that will not require tightly synchronized clocks

5. **Intelligent Nodes**: Nodes will have the ability to detect/mitigate wormhole by themselves
6. **Mobile/Non Static Nodes**: We need to allow nodes mobility also.
7. **Detect ALL types** of wormholes: Need to detect all types of wormhole attacks (e.g. hidden and exposed)
8. **Pinpoint the attackers**: Need to identify the attackers also.
9. **Avoid/Prevent Detect AND Mitigate**: Most of the solutions, avoid detect or mitigate. Most of them do not take into account all the three dimensions. In the first line of action we need to prevent wormholes i.e. do not allow them to occur at all (Avoid). Then we need to detect it; incase a wormhole was already present in the network (detect). And when wormhole found we need to punish the attackers i.e. we need to detect the attackers also and neutralize the effects of wormhole attack (mitigate).
10. **No specialized nodes**/CA/Normal Network: Finally, nodes must be able to work independent of other nodes for detection of wormhole in the network.

We need a solution that can achieve all of the Objectives mentioned above. A hybrid solution is inevitable that has the ability to achieve all these goals.

As a future work, we are hereby proposing a solution that will be novel, simple, and efficient and will have the ability to achieve most of the above goals; if not all. For the exposed wormhole problem we have already detected it by using Routing Table and neighbor verifications [36]. And for the hidden type of wormhole attack we will be using a combination of Received Signal Strength Indicator (RSSI) and the Round Trip Time (RTT). We know that obtaining a complete solution won't be without some extra costs, what we will be doing in future is to asses these costs and comparison of our solution to existing solutions.

5 REFERENCES

[1] Hu, Y.-C.; Perrig, A.; Johnson, D.B.; , "Packet leashes: a defense against wormhole attacks in wireless networks," INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies , vol.3, no., pp. 1976- 1986 vol.3, 30 March-3 April 2003

[2] Oluoch, Jared, et al. "A simulation study of impacts of collaborative wormhole attacks in mobile ad hoc networks (MANETs)." Proceedings of the 2012 Information Security Curriculum Development Conference. ACM, 2012.

[3] Dhurandher, Sanjay Kumar, et al. "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks." Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on. IEEE, 2012.

[4] A.Vani, D.Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), 2011, Vol. 3 No. 6, pp. 2377-2384, June 2011

[5] S.Vijayalakshmi and S.Albert Rabara. Article: Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques - LP3 and NAWA2. International Journal of Computer Applications 16(7):26–33, February 2010

[6] Khalil, I.; Saurabh Bagchi; Shroff, N.B.; , "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on , vol., no., pp. 612- 621, 28 June-1 July 2005

[7] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W.; , "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, 2005 IEEE , vol.2, no., pp. 1193- 1199 Vol. 2, 13-17 March 2005

[8] Maheshwari, R.; Jie Gao; Das, S.R.; , "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , vol., no., pp.107-115, 6-12 May 2006

[9] Meghdadi M, Ozdemir S, Güler I. A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks. IETE Tech Rev 2011;28:89-101

[10] Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C.; , "DoS Attacks in Mobile Ad Hoc Networks: A Survey," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , vol., no., pp.535-541, 7-8 Jan. 2011

[11] J. Eriksson, S. Krishnamurthy, and M. Faloutsos. "Truelink: A practical countermeasure to the wormhole attack," International Conference on Network Protocols, pp.75−84, Nov. 2006.

[12] A. Malhotra, D. Bhardwaj, and A. Garg, "Wormhole attack prevention using clustering and digital signatures in reactive routing", ;in Proc. ICNSC, 2012, pp.122-126.

[13] Srdjan Čapkun , Levente Buttyán , Jean-Pierre Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, October 31, 2003, Fairfax, Virginia

[14] Weichao Wang , Bharat Bhargava, Visualization of wormholes in sensor networks, Proceedings of the 3rd ACM workshop on Wireless security, October 01-01, 2004, Philadelphia, PA, USA

[15] L. Lazos and R. Poovendran, "Serloc: Secure range-independent localization for wireless sensor networks," Proceedings of the ACM Workshop on Wireless Security, pp. 21−30, Oct. 2004.

[16] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks", Proc. Symp. Netw. Distrib. Syst. Security, 2004

[17] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.P. Hubaux. "A practical secure neighbor verification protocol for wireless sensor networks," ACM WiSec, 2009.

[18] Honglong Chen , Wei Lou , Xice Sun , Zhi Wang, A secure localization approach against wormhole attacks using distance consistency, EURASIP Journal on Wireless Communications and Networking, 2010, p.1-11, April 2010

[19] Hazra, Swarnali, and S. K. Setua. "Trusted Routing in AODV Protocol Against Wormhole Attack." Future Information Technology, Application, and Service(2012): 259-269.

[20] Zhang, Ting, Jingsha He, and Yang Zhang. "Secure DV-Hop

Localization against Wormhole Attacks in Wireless Sensor Networks." Soft Computing in Information Communication Technology (2012): 33-38.

[21] Keerthi, T., and Pallapa Venkataram. "Locating the Attacker of Wormhole Attack by Using the Honeypot." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.

[22] Vijayalakshmi, S., and P. Annadurai. "Arresting Wormhole Attack in Ad hoc Network using Cumulative Threshold Transmission Rate." International Journal of Computer Applications 54.18 (2012).

[23] 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.

[24] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.P. Hubaux. "Secure neighborhood discovery: A fundamental element for mobile ad-hoc networking," IEEE Communications Magazine, Feb. 2008.

[25] M. Poturalski, P. Papadimitratos, and J.P. Hubaux. "Secure neighbor discovery in wireless networks: Formal investigation of possibility," ACM ASIACCS2008, pp. 189−200, 2008.

[26] Sakthivel, T., and R. M. Chandrasekaran. "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach." European Journal of Scientific Research 76.2 (2012): 240-252.

[27] Reddy, K., and P. Thilagam. "Intrusion Detection Technique for Wormhole and Following Jellyfish and Byzantine Attacks in Wireless Mesh Network."Advanced Computing, Networking and Security (2012): 631-637.

[28] Zhang, Yu, and Xin Feng. "Ad Hoc LAN Protocol-Based Defense Wormhole Attack Method." Recent Advances in Computer Science and Information Engineering (2012): 195-201.

[29] P.V. Tran, L.X. Hung, Y.K. Lee, S. Lee, and H. Lee. "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks," 4th IEEE Consumer Communication and Networking Conference (CCNC'07), pp. 593−8, May 2007.

[30] Venkataraman, Revathi, et al. "A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks." International Journal of Recent Trends in Engineering 1.2 (2009).

[31] Raju, V. Karthik, and K. Vinay Kumar. "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks." Computing Sciences (ICCS), 2012 International Conference on. IEEE, 2012.

[32] Khalil, S. Bagchi, and N.B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks," Elsevier Ad Hoc Networks, vol. 6, no. 3, pp. 344−62, 2008.

[33] Song, Sejun, Haijie Wu, and Baek-Young Choi. "Statistical wormhole detection for mobile sensor networks." Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on. IEEE, 2012.

[34] Jain, Shalabh, and John S. Baras. "Preventing wormhole attacks using physical layer authentication." Wireless Communications and Networking Conference (WCNC), 2012 IEEE. IEEE, 2012.

[35] Upadhyay, Saurabh, and Brijesh Kumar Chaurasia. "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach." Advances in Computer Science and Information Technology. Networks and Communications (2012): 402-408.

[36] Khan, Zubair Ahmed, and M. Hasan Islam. "Wormhole attack: A new detection technique." Emerging Technologies (ICET), 2012 International Conference on. IEEE, 2012.

[37] R. Venkataraman, M. Pushpalatha, T.R. Rao, and R. Khemka. "A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad-hoc networks," International Journal of Recent Trends in Engineering, vol. 1, no. 2, May 2009.

[38] S. Jain, T. Ta, J. S. Baras, "Wormhole Detection Using Channel Characteristics", Proceedings of the First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), Ottawa, pp. 2712-2717, Canada, June 10-15, 2012.

[39] Jaiswal, Ranjeet, and Sanjay Sharma. "Relative Cluster Entropy Based Wormhole Detection Using AOMDV in Adhoc Network." Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. IEEE, 2012.

[40] Banerjee, Subhashis, and Koushik Majumder. "A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network." Recent Trends in Computer Networks and Distributed Systems Security (2012): 372-384.

[41] Modirkhazeni, Ali, et al. "Mitigation of Wormhole Attack in Wireless Sensor Networks." Trustworthy Ubiquitous Computing (2012): 109-147.

[42] Sadeghi, Mohammad, and Saadiah Yahya. "Analysis of Wormhole attack on MANETs using different MANET routing protocols." Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on. IEEE, 2012.

[43] 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

[44] Maulik, Reshmi, and Nabendu Chaki. "A study on wormhole attacks in MANET." International Journal of Computer Information Systems and Industrial Management Applications ISSN (2011): 2150-7988.

[45] Simsek, Oya, and Albert Levi. "A Distributed Scheme to Detect Wormhole Attacks in Mobile Wireless Sensor Networks." Computer and Information Sciences II: 26th International Symposium on Computer and Information Sciences. Springer, 2011.

[46] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "MANET: Vulnerabilities, Challenges, Attacks, Application." International Journal of Computational Engineering & Management 11 (2011): 32-37.

[47] 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.

[48] Song, N.; Qian, L.; Li, X.; , "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, vol., no., pp. 8 pp., 4-8 April 2005.