Journal of Computer Science 9 (12): 1626-1637, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1626.1637 Published Online 9 (12) 2013 (http://www.thescipub.com/jcs.toc)

PERFORMANCE EVALUATION OF WORMHOLE SECURITY APPROACHES FOR AD-HOC NETWORKS

[1]Ismail Hababeh, [2]Issa Khalil, [3]Abdallah Khreishah and [4]Samir Bataineh

[1]Faculty of Computer Engineering and Information Technology, German-Jordanian University, Jordan
[2]Qatar Computing Research Institute (QCRI), Qatar Foundation, Doha, Qatar
[3]Newark College of Engineering, New Jersey Institute of Technology, Newark NJ, USA
[4]Faculty of Information Technology, United Arab Emirates University, UAE

Received 2013-08-15, Revised 2013-10-12; Accepted 2013-10-29

ABSTRACT

Ad-hoc networks are talented but are exposed to the risk of wormhole attacks. However, a wormhole attack can be mounted easily and forms stern menaces in networks, particularly against various ad-hoc wireless networks. The Wormhole attack distorts the network topology and decrease the network systems performance. Therefore, identifying the possibility of wormhole attacks and recognizing techniques to defend them are central to the security of wireless networks as a whole. In this study, we will summarize state of the art wormhole defense approaches, categories most of the existing typical approaches and discuss both the advantages and disadvantages of these methods. We will also point out some unfulfilled areas in the wormhole problem and provide some directions for future exploring.

Keywords: Ad-Hoc Networks, Security, Wormhole

1. INTRODUCTION

With the growth of wireless technology, ad hoc networks have been developed into many forms. However, the security issue is one of the major bottlenecks, which restrict the further development of ad hoc networks (Papadimitratos and Haas, 2002). The open nature and multi-hop routing characteristics lead the security issues to be hard to avoid. Among all of the possible attacks, wormhole is common attack in ad-hoc networks and causes serious security problems, since it can destroy the normal work of the whole network (Hu *et al*., 2006).

Normally, in a wormhole hit, an adversary obtains packets at one place in the network and then, maliciously transmits the packets to another place and replays them into the network. In most cases, the forwarded packets are received by other adversaries who transmit them cruelly to other network places which in turn harm the network security (Ramaswamy *et al*., 2003; Sen *et al*., 2007). However, in some cases, the adversary itself can launch the attacks via higher power broadcast, or by out of band channel. Moreover, wormhole attacks are known as tunneling in some research in the literature and the link or tunnel between the both end positions of a wormhole is called wormhole link, or wormhole tunnel.

Wormhole attacks can be initiated in several types. In our research, we classify them into three categories, namely, hardware attacks, broken protocol wormhole attack and malicious protocol. In hardware based attacks, the attacker can use out-of-band channel, or use higher transmitting power to make a wormhole in network. For example, we assume two adversaries (A) and (B), they somehow establish a communication link between them. This link can be an extended range track wireless link, or a wired cable.

Whenever, (A) heard data in his neighborhoods, it will directly forward this data through the out-of-band link to the adversary (B) and B in turn will broadcast them to B's neighbors. No matter the data packets be encrypted, or decrypted, it have been transmitted to the other places with a faster speed than purely using the original network. As for the attacks using higher

Corresponding Author: Ismail Hababeh, Faculty of Computer Engineering and Information Technology, German-Jordanian University, Jordan

transmission power, whenever a nasty node heard a routing demand, it will broadcast the demand with a higher power. By this way, the node has more chance to distort the network, since some non-neighbor nodes may also receive these packets and consider the malicious nodes as neighbors.

In broken protocol based wormhole attacks, the malicious nodes don't follow the requirements of specific protocols during data transmission. For example, if a protocol requires all nodes need to be rear for a arbitrary time before forwarding packets in order to reduce the collision, the adversary can just broadcast the data once it receive them. By this way, the adversary can let the path in which it contained faster than others (Jain and Kandwal, 2009).

In the malicious protocol attacks, the adversary may use its own protocol to change the data packets during transmitting. The most typical wormhole attack of this type is encapsulation where a nasty node is located somewhere in the network and heard a routing request. Then, it put a special tag in the data and forwards it to a far away collude adversary node. This adversary will delete all data packets which are located between the first adversary and the second. Moreover, the second malicious node will broadcast the modified data to its neighbors. When this routing request reaches its destination, the receiver may regard the path in this modified packet as the fastest routine and send it back to the request initiator. In contrast, the sender will use this path to send its data, rather than the real shortest routing.

The influence of wormhole is huge. If a wormhole is sited cautiously by the adversary and the length of wormhole link is adequate, the link then can absorb a bunch of routes, which may cause many further serious security issues. A menace wormhole attack that threatens network security is known as black-hole in which the adversary deletes all the data packets sent through the tunnel (Arora *et al*., 2010; Tamilselvan and Sankaranarayanan, 2007). However, if the wormhole link is small, it doesn't draw too many routing traffics, but it still affect the quality of service in local regions.

In a normal wormhole attack, the adversary attempts to convince other network nodes that there exists a path between two locations, but in fact there is no path between the nodes. Such scenario is known as exposed wormhole (Poovendran and Lazos, 2007) where the non-adversary nodes can detect the existing nodes which are directed by the adversary. The other nodes treat the wormhole end nodes as normal nodes and they will directly forward the packets to them if they are neighbors.

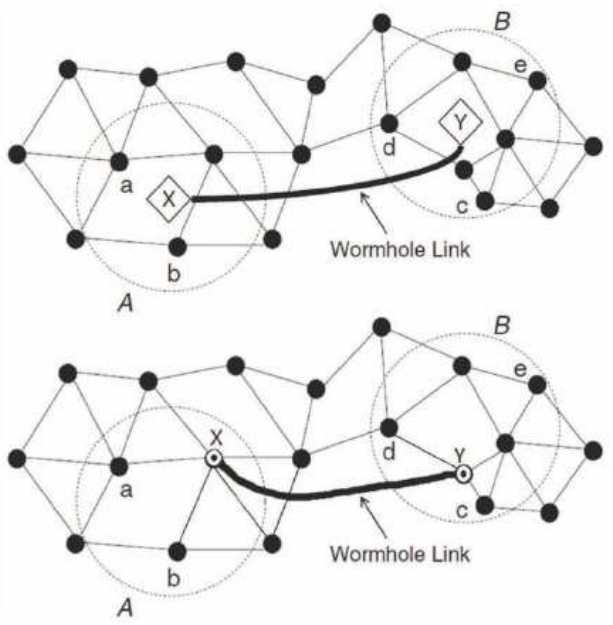


Fig. 1. Exposed and hidden wormhole scenarios

On contrast, if the other nodes do not know the location of such wormhole nodes, this scenario is known as hidden wormhole.

Figure 1 depicts the exposed and hidden wormhole scenarios. The wormhole nodes just replicate the wireless signals in the air and forward it through a tunnel.

Several methods in the literature are discussed the wormhole detections in ad hoc networks. Statistic wormhole detection (Zhao *et al*., 2010) and wormhole detection with multi-dimensional scaling (Perrig *et al*., 2000) are two typical defense approaches.

As for the centralized mechanism, a central server, or node, is responsible for collecting related information from the whole networks and consequently build some global interpretations. An algorithm is used in this technique to check the abnormal or inconsistent interpretations.

In ad hoc networks, statistic techniques assume that the distribution of nodes follow certain kind of mathematical distribution. However, with existing of the wormholes, the number of each node's neighbors and the shortest length between each two nodes will not satisfy the mathematical distribution model and so it can be inferred the presence of wormholes in a network. However, the ad-hoc always relay on the assumption that the nodes distribution can be obtained in normal cases.

The multi-dimensional scaling based wormhole detection approach applies MDS-VOW algorithm to construct a virtual layout of the networks. If the network is attacked by a wormhole, the structure of the network must be changed. However, this method depends on the nodes neighborhood information; each node needs to obtain its neighborhood table periodically, even if there is not data packet transmit between them. As the power in ad hoc network is limited, transmitting the whole neighboring information is not a good and practical solution.

In the distributed wormhole detection approaches, each node collects its k-hops neighbor's information (Sanzgiri *et al*., 2002). Based on this information, each node finds the locations of some affected regions caused by wormholes and stop forwarding packets which came from those regions to isolate the wormhole (Nasipuri *et al*., 2001; Pirzada and McDonald, 2004). The distribution wormhole detection algorithm can be further classified into two approaches, namely, non-routing neighboring monitoring based approach (Huang and Lee, 2003) where each node monitors the topology structure of its neighbors (Wang *et al*., 2010; Maheshwari *et al*., 2007), or the inputs and outputs data flows (Khalil *et al*., 2005; 2008) and routing receiver monitoring based approach where a data packet is monitored by the nodes in its routine. The typical distributed approaches are packet leashes (Hu *et al*., 2003; 2006), TESLA with Instant Key-disclosure (Perrig *et al*., 2000) and mutual authentication with distance-bounding (Liu *et al*., 2005; Du *et al*., 2006).

The remainder of the study is organized as follows: Section 2 describes some centralized statistical techniches and section 3 depicts multi-dimensional scaling approaches. Distributed wormhole defense technologies are presented in Section 4. Finally, Section 5 draws conclusions and outline future work.

2. CENTRALIZED STATISTICAL WORMHOLE DETECTION

Two statistical based wormhole defense approaches will be described, namely, SA-TC and MDS-VOW. SA-TC approach presented in (Zhao *et al*., 2010) computes the distribution of a link being used in different routings. The SA-TC approach implies that a wormhole attack can be detected by using some statistical formulas where routing significantly differ from the normal status.

In general, the SA-TC approach composed of three parts; analyzing routing information; determining the uncertain link set and validating with time limitation. As this approach is used in wireless sensor network, there is at least one sink node to collect data. This sink node is responsible for gathering the routing information from all sensor nodes.

Initially, each node works as a sender and will send its routing information {Rij} to the other nodes in the networks. Then, the sink node will collect these {Rij} from all nodes and compute the time of the direct link between two neighbors appears in R. Based on this, the sink node can obtain the statistical information about time of a link being used. Based on the characteristics of wormhole hits, as the majority of broadcast capacity is engrossed into the wormhole links, the time of the wormhole being used will be highly increased. **Figure 2** illustrates a normal ad-hoc network system statistics against a wormhole attacked ad-hoc network system.

The SA-TC technique is periodically computes the distribution about links' usages and then, treats the links used more frequent than the average frequency in safe-condition as suspicious links. The suspicious links set is refined by finding the link with more difference. The fake link has a better performance to absorb increasing transmission volume, but the real transmitting time of real data packets will be prolonged. The SA-TC technique sends some probe messages to nodes where the suspicious links began and then calculates the real transmission time through the suspicious links. Through this way, the locations of wormholes are detected.

Another method of detecting wormhole attacks is proposed and works as follow: a central server is used to collect neighborhood tables and the routing tables and then, it computes the degree of nodes distribution in the network and the length of shortest path between any two nodes. However, this method can only detect a wormhole attack in a network, but failed to provide solutions to isolate the wormhole.

The statistical approaches assume there is a way to obtain the nodes distribution under the conditions of no adversaries. However, this assumption is not piratical in the real world, since during building up the network, the malicious nodes can be deployed.

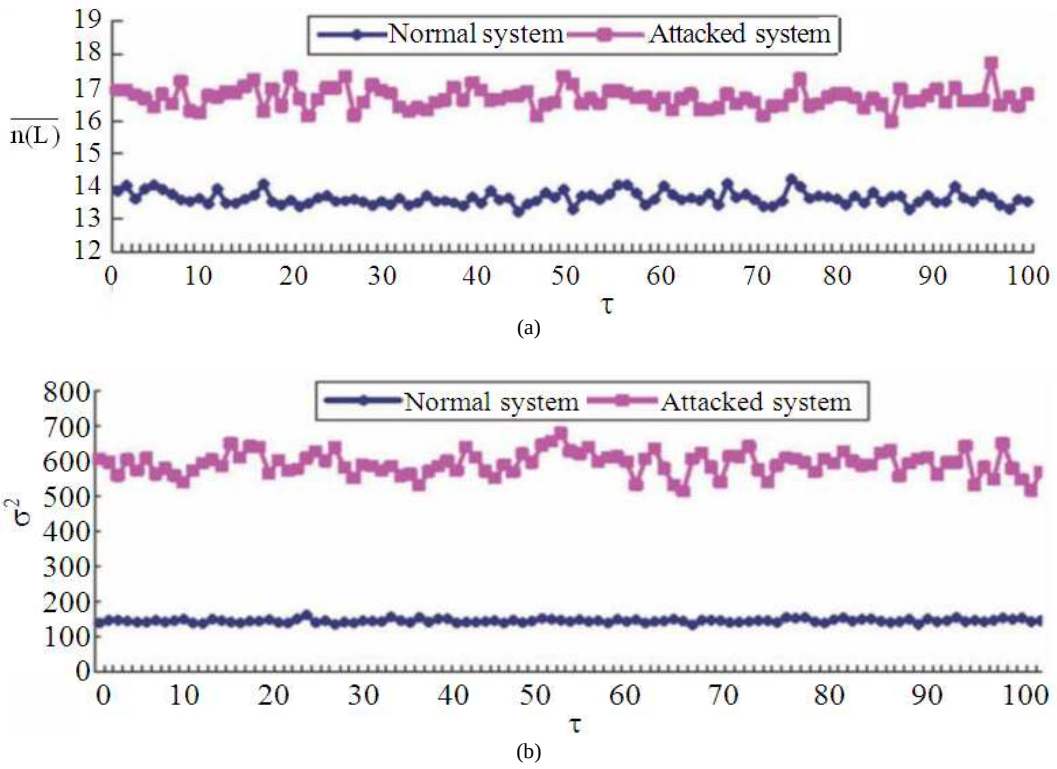


Fig. 2. Statistic-based wormhole detection (a) $\overline{n(L)}$, (b) $\sigma^2(\{n(L_{ij})|\forall L_{ij} \in L\})$

3. MULTI-DIMENSIONAL SCALING APPROACHES

MDS-VOW technique is a Multi-dimensional scaling approach (Wang and Bhargava, 2004). It is centralized wormhole detection technique based on augmenting the connectivity information with estimated distance between the nodes being neighbors. The key point of this method is to build a virtual design of the network and then, to find the inconsistencies in it. Since the network is built in plane, the reconstructed layout also ought to be a structure in the plane.

However, with the existing of wormhole, which shortens the virtual distance between two locations, the rebuilt layout will become a curly structure. MDS-VOW algorithm is designed to process the collected data and to make the virtual network layout. By further analyze the virtual layout, the distortion can be located by identifying the affected nodes, like finding the position where the distortion began. However, the weak side of this method is the computing complexity as we need to collect plenty of data and also to build a virtual network layout in three-dimensions.

4. DISTRIBUTED WORMHOLE DETECTION

Most of the distributed approaches detect wormhole attacks by two ways: Either by checking some forbidden structure in networks, or monitoring the flows of neighbor nodes.

Maheshwari *et al*. (2007) proposed a wormhole defense technique that utilizes connectivity information to search for prohibited compositions in the connectivity graph. Specifically, it looks for graph structures that prohibit a Unit Disk Graph (UDG) insertion, thus it cannot be presented in an authorized connectivity graph. Due to the fact that the complexity of looking for UDG embeddings is NP-hard problem, this technique cannot promise to discover the wormhole in all cases.

However, MDS-VOW is relatively simple and it can also provide a significant wormhole recognition probability in ad-hoc networks. This technique is based on two lemmas about disk packing. The first lemma: within a predetermined region, a set of nodes can't be grouped unless there exist edges between them. They

first consider the case that two non-one-hop neighbors' sensing range has intersections and mentioned that inside the intersection region, at most, we can set two non-one-hop nodes. If the region has a wormhole, then the number of non-one-hop nodes in the intersection may greater than two. By finding such forbidden structure, we can identify the wormhole affected areas.

In order to clearly the second lemma, we need to restate the symbols used in MDS-VOM: p(S, r) denotes the upper limit number of points in a region S, such that the distance between every pair of points in S is greater than r; DR (u) is used to represent a disk region of radius R, centered at node u. Moreover, L(r, R) = DR(u) ∩ DR (v) represents the intersection of the two disk regions, whose radius are R and are centered at u, v with distance r between them. When R = r = 1, only L is denoted. Therefore, the first lemma can be written as p(L, 1) = 2.

The second lemma is about the forbidden structures among k-hop neighbors:

$$p(L(r,R),\beta) \le \left\lfloor \begin{array}{l} \frac{8}{\pi}\left(\frac{R}{\beta}+\frac{1}{2}\right)^2 \times \arccos\left(\frac{r}{2R+\beta}\right) \\ -\frac{4r}{\pi\beta^2}\sqrt{\left(R+\frac{\beta}{2}\right)^2-\frac{r^2}{4}} \end{array} \right\rfloor, \text{for } r \le 2R$$

Lemma 2 provides the loss bound for the maximum number of β-hop neighbors. It is assumed that the upper limit number of autonomous ordinary β-hop neighbors for two non-neighboring nodes is smaller than the right side of Lemma 2.

After providing the two lemmas, the conditions which broke both Lemma 1 and Lemma 2 are stared, as the forbidden structures. The wormhole detection method is constructed as follows: each ad-hoc node maintains a 2k-hop neighboring table, named N_{2k} (u). In each time, the node (u) picks up a non-neighboring node, (v), from its neighboring table and computes the ordinary k-hop neighbors C_k (u, v). After obtained all of the common k-hop neighbor set of node u, u will compute the maximum independent set by a greed algorithm: starting from an empty set, in each time, the algorithm first picks a random node and includes it in the autonomous set, then, removes its neighbors. This process is continued until there are no nodes in C_k (u, v) and the resultant set is the most independent set of node u. If the volume of u's independent set is greater than the number indicated by lemmas, then node u is influenced by a wormhole.

The nodes which are located in the broadcast radius of the wormhole nodes are defined as corrupted nodes. In order to isolate the wormholes, the corrupted nodes are removed from each node neighbor lists such that the tunneled packets cannot be forwarded. **Figure 3** depicts the wormholes detection and isolation process.

Wang *et al*. (2010) proposed a similar wormhole detection and isolation approach. The proposed approach is mainly based on the following corollary: If there exist three mutually non-one-hop neighbor nodes in the intersection area of the two-hop neighbor sets of the nodes p and q, then p and q are certainly affected by a wormhole. Based on this corollary, a WDI algorithm is introduced, which also isolates all the suspicious nodes.

This method presents performance analysis in mathematical formulas. With reference to spatial statistics hypothesis in (Cressie, 1992; Farago, 2002), the Poisson distribution can be obtained by set up an arbitrarily number of consistent nodes in a region. The probability that a region S contains k nodes can be computed as follows, where ρ represents is the density of a given network:

$$P(|S|=k) = \frac{(\rho S)^k}{k!} \in^{-\rho S}$$

Since this method is based on the number of non-one-hop neighbor nodes in the common circle areas, the number of nodes in the intersection region directly determines the probability of detecting a wormhole. If we assume that the size of intersection is S where ($S = \alpha\pi R^2$), then the previous formula can be transformed into a new one as follows:

$$P(|S|=k) = \frac{(\rho S)^k}{k!} e^{-\rho S}$$

$$= \frac{\left(\frac{n}{\pi R^2} \times \alpha\pi R^2\right)^k}{k!} e^{-\frac{n}{\pi R^2}\times\alpha\pi R^2} = \frac{(n\alpha)^k}{k!} e^{-n\alpha}$$

The low bound of detecting probability is considered in this case. **Figure 4(a, b)** depicts the probability of detecting wormholes in a minimum of 3 non-one-hop neighbors in a circle, 4(a) shows the worst case. The area of the strapped region is computed by:

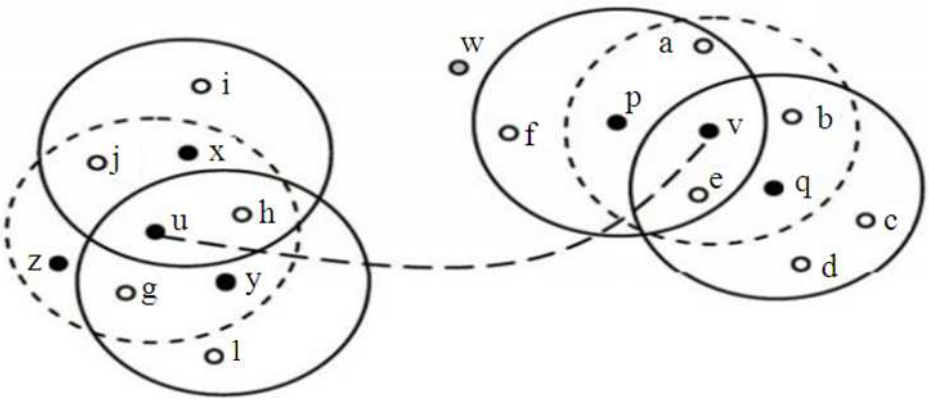
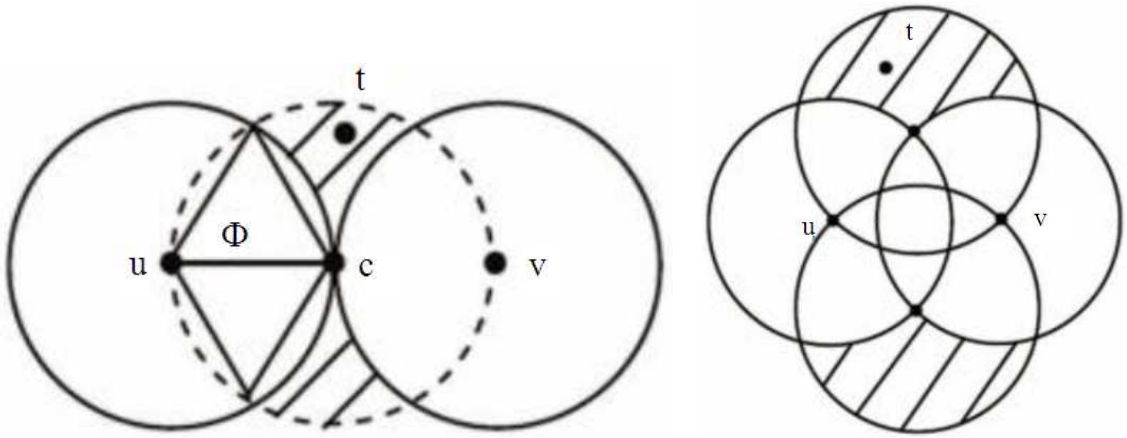


Fig. 3. Wormhole detection and isolation



(a) (b)

Fig. 4. The probability of detecting wormholes, (a) $d_{uv} = R$, (b) $d_{uv} \in [R, 2R]$

$$S_{shad} = \pi R^2 - 2\left(2R^2 \cos^{-1}\left(\frac{1}{2}\right) - R^2 \sin\left(\cos^{-1}\left(\frac{1}{2}\right)\right)\right)$$

If n is the average number of nodes in a circle, then the probability of existing more than one node in the strapped area is computed as follows:

$$P_{shaded} = P\left(|S_{shaded}| \geq 1\right) = 1 - P\left(|P_{shaded}| = 0\right) = 1 - e^{-0.218n}$$

Accordingly, if the average number of a node's one-hop neighbors is estimated to 10, then wormhole sensing probability of the WDI is closed to 100%.

This method detects both exposed wormholes and hidden wormholes. However, it can't successfully find out all the wormholes in the network. In addition, if the adversary puts the wormhole sophisticatedly, it may lead to network disconnections. Moreover, this method is not applicable for high dynamic scenarios.

The LiteWorp method (Khalil *et al*., 2005) is developed for wormhole detections. This method uses guard nodes to monitor the input and output flows of their neighbors. If B and C are neighbors of node A and B is the previous hop node of C, then, node A is able to watch the link from B to C and C is the node been monitored. Each guard node has a watch buffer which saves the information from all the packets sent through the monitored links. In this buffer, there is time stamp (t) to record the packets' incoming and leaving times in each monitored node, which means C must forward the packet, sent from B, within a time threshold. A malicious counter MalC(i,j) is retained for all guarding nodes. Once the guard node i detects that the monitored node j

fails to transmit a packet within the threshold, the malicious counter will be increased. There is another threshold, MalCth, which is used to determine the suspected malicious nodes. When the growing values in malicious counter becomes greater than MalCth, the guard node i will cancel the monitored node j from its neighbor list and sends an authenticated aware message to the neighbors of j. The aware message indicates that the node j is a assumed nasty node.

For the sake of security, after a neighbor of j, assuming k, gets the alert message, it will verify two things by authentication: the guard node (i) is one of the first-hop neighbors of j and j is k's neighbor. Without the authentication steps, the adversary may fake some guard nodes to send malicious alter messages, which can frame other pure users.

After the authentication steps, node k will store the characteristics of j in an aware buffer. When k obtains sufficient aware messages about j, k will revoke j from its neighbor list and add j into a local blacklist. The blacklist is designed to maintain memories about malicious nodes in order to guarantee that the malicious nodes cannot become the neighbor nodes of k in later.

Although LiteWorp can identify and separate the wormhole nodes, but it still has some restrictions. It is only suitable for static scenarios. As an improvement to this method, a new method MobiWorp (Khalil *et al*., 2008) is developed. MobiWorp has two types of detections. The first type is called local detection that has local checking on neighborhood communication. The second type is called global detection which depends on a protected Central Authority (CA) to follow up the position of portable nodes. The isolation in MobiWorp is attained locally where the nasty node is deleted from the existing neighborhood and globally where CA can continuously forbid the malicious nodes.

In the local phase, it is assumed that every node identifies its one-hop and two-hop neighbors. When a packet being forward by a node, the sender should also announce the node whose send the current packet. As an example, a pair of colluded adversaries is assumed, M1 and M2. After M2 received a routine request query packet tunneled from M1, the adversary M2 only has two options to further forward the packet: announce the identity of M1 as the packet sender, or announce the characteristics of a single M2 neighbors, assuming X, as the packet sender.

In the process of local revocation, if M1chooses the first option, then all M2 fellows will refuse the routine request, since M1 is not a fellow of M2. If the adversary uses the second option, then, all the guard nodes (neighbor nodes) of both nodes X and M2 will detect that M2 fabricated the route request, since they did not find corresponding data from X. When a neighbor detects one of the above two cases, it will report the abnormal event to CA and it will also send revoke message to the neighbors of M2. The CA will record these local revocations of the corresponding nodes.

Being different from LiteWorp, MobiWorp assumes that each mobile node can predetermine its destination before the real movement and that the mobile nodes also contain some localization devices, such as GPS (Hofmann-Wellenhof *et al*., 1993). An Authentication Neighbor Update Message ANUM is used. It is a logical location certification given by the CA. In this system, a node cannot forward any packet without the ANUM. The basic idea of this designation is that a node can't initiate a wormhole without forward any traffic information.

The ANUM is bounded by the logical position of a node and the active instance. The ANUM is valid only when the actual position of the current node is actually in the ANUM's bounded region and the current forwarding time is smaller than the ANUM's expired time. In CA, if the total number of local revocations of a node, assuming Y, is greater than a pre-defined threshold, the CA will revoke the Y's ANUM and will no longer send ANUM to it. Since Y does not have ANUM, it cannot forward any packet in the network and therefore, the wormhole maker is blocked forever.

Although the MobiWorp detect the wormhole nodes locally, the final isolation is made by a centralized CA. Hence, the MobiWorp is a mixture of both centralized and decentralized wormhole defense method. Besides the centralized characteristic, the nodes in MobiWorp also need to be equipped with some localization devices and the proposed solution requires each node to update ANUM from CA, which may cause a lot of extra energy.

Hu *et al*. (2006) described the geographical and chronological packet leashes for wormhole detection. They design an authentication protocol, named TIK, in order to guarantee that the temporal leashes cannot be modified.

In general, a leash is additional information on a packet that intended to limit the packets' upper limit broadcast distance. Hence, the geographical leashes are the distance bound, which limits the maximum distance a packet can get from the sender, while the chronological leashes are the time bound, which indicate the lifetime of

packets. In this technique, every node should have either precise localization device or an accurate clock for synchronization.

To create a geographical leash, every node must recognize its location, which can be obtained by using GPS or some other localization technologies. In this method, loosely synchronized clocks are considered. When sending a packet, the network system will add the sender's location, p_s and the sending time, t_s, with the packet.

After receiving such a packet, the receiver node will compute its position, p_r and the receiving time, t_r. The distance between the sender and the receiver is computed as follows: if the variation among sender's clock and receiver's clock is Δ and the maximum velocity of a node is v, then, the real distance between sender and receiver, the highest transmitting distance of a packet d_{sr} can be computed as follows:

$$d_{sr} \le \| p_s = p_r \| + 2V \times (t_r - t_s + \Delta) + \delta$$

where, ||ps-pr|| is the reported distance between sender and receiver; $2V \times (t_r - t_s + \Delta)$ is caused by the movements of both sender and the receiver; δ is measurement errors of localization device. After computing the d_{sr}, the sender node will add the geographic leash with the data and send it to the receiver. If the packet is tunneled to some other faraway places, the receiver will detect the inconsistence and drop the packet.

To create a chronological leash, every node should have firmly synchronized clock that can be realized by LORANC (Mills, 1992), or WWVB (Lombardi *et al*., 2005). The sender should comprise the sending time, t_s with the packet, while the receiver first check the receiving time, t_r, with t_s. If the V_{light} represents the speed of light and Δ_t is the error of time measurement, then the maximum distance between sender and receiver, d′, should satisfy the following formula:

$$d' \le V_{light} \times (t_r - t_s + \Delta_t)$$

The wormhole detection can be carried out by two ways; the receiver detects whether the packet traveled too far by considering the relation between V_{light} and the sender can add an expiration time with the packet:

$$\frac{\| p_s - p_r \| - \Delta_t}{t_s - t_r}$$

The leash based approaches assume that the packets delay in sending, processing and receiving are negligible. In order to guarantee the accuracy of the information in the leashes, the geographical and chronological leashes need to include data verification. Normally, the Merkle hash tree based authentication scheme is used (Merkle, 1980). **Figure 5** illustrates the Merkle hash tree.

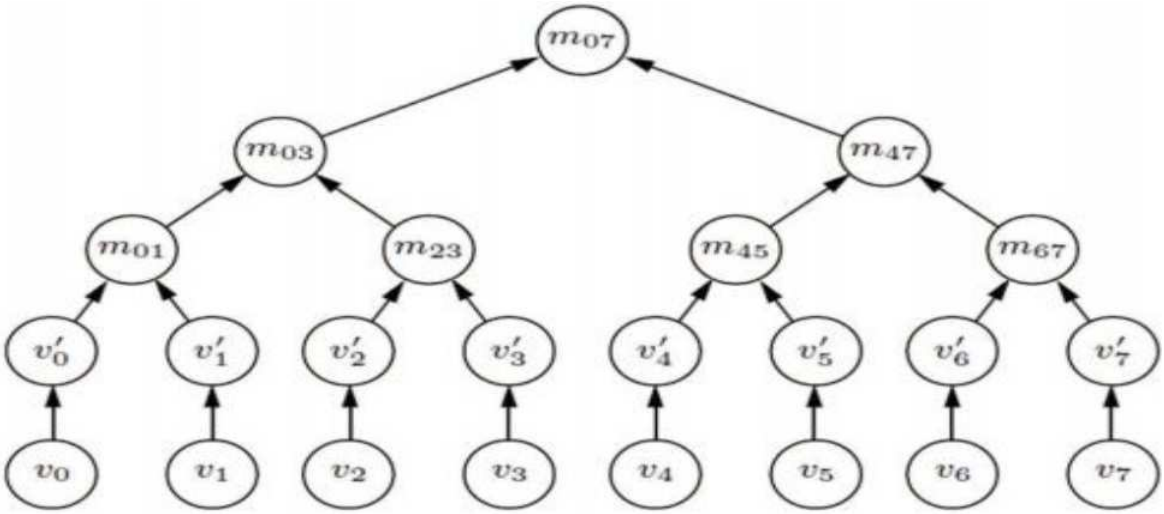


Fig. 5. The merkle hash tree

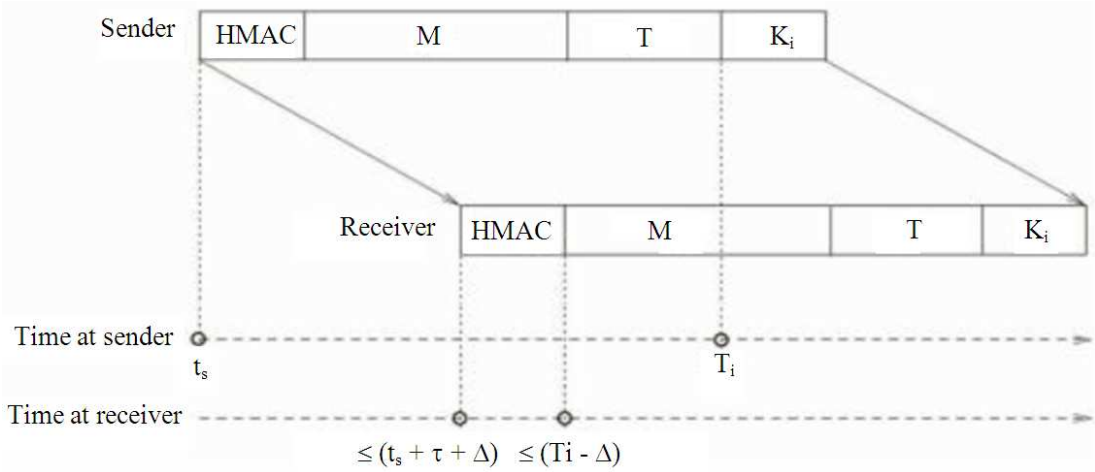


Fig. 6. The time sequence in TIK protocol

TESLA with Instant Key disclosure (TIK) is an extension of the TESLA authentication protocol (Perrig *et al*., 2000) that implements chronological leashes in wireless networks. The new idea of TIK is that the packet broadcast time can be greater than the time synchronization error (Hu *et al*., 2006). In such cases, the packet receiver can authenticate the TESLA security state; this reality allows the sender to reveal the key in the same packet, therefore motivating the TESLA protocol with instant key disclosure. **Figure 6** depicts the time sequence in TIK protocol.

In TIK protocol, the packet transmitted by a sender, S, is defined as < $HMAC_{Ki}$ (M), M, T, Ki >, where $HMAC_{Ki}$ (M) represents a HMAC value of message M; T represents other hash tree's values, which will be used for validation; K_i represents the key for time period from T_i-1 to T_i (Bellare *et al*., 1996). Prior to send a packet (P), the sender approximate the upper bound t_r on the entrance time of the HMAC at the receiver. Based on the computed receiving time, the sender will pick a key K_i, which will not expire before the receiver obtains the packets HMAC, to compute the hash value of the message. After computing $HMAC_{Ki}$ (M) with K_i, the sender appends the HMAC to the packet. When the key expired, the sender releases the key K_i, assailant can't change the HMAC value of the sending data as K_i is not known.

When receiving a packet, the receiver should first verify that the corresponding key has not finished. Then, after the receiver gets the key of the current packet, it further authenticates the key by using the root value of the Merkle tree, m and the other hash tree value T. Then, it uses the authenticated K_i to validate the HMAC value in the packet. Finally, if no incorrect values are occurred, the receiver recognizes the packet as the genuine data. TIK protocol assured that the wormhole broadcasts the packets gradually and not faster than the typical routes. Hence, when the receiver obtains a wormhole tunneled packet, the corresponding key is already expired. Although the TIK protocol affords security against the wormhole attack, it results in more delay. However, the conditions of TIK are also unfeasible where it supposes that the packet sending and receiving delays are negligible and the sender can obtain the positions of all nodes in the network.

Wang *et al*. (2010) and Prasannajit *et al*. (2010) independently presented two similar wormhole detection approaches. Both of them use local multidimensional scaling and hop-coordinates (Xu *et al*., 2006). The proposed wormhole detection algorithm in (Prasannajit *et al*., 2010) is built on Round Trip Time (RTT) and geographic distance. This algorithm detects the wormholes in two steps. The first step is based on a hop counting technique and uses the RTT as a probe, each node in the network can collect a group of hop counts of its neighbor nodes that are within one/k hops from it and also obtain another group of hops based on the RTT of the message between consecutive nodes and their neighbor numbers. In the second step the network is reconstructed locally by MDS algorithm, the node first runs Dijkstra algorithm to get the shortest path for each pair of nodes, based on hoping count and RTT individually and then, rebuild a local map using Multidimensional Scaling (MDS).

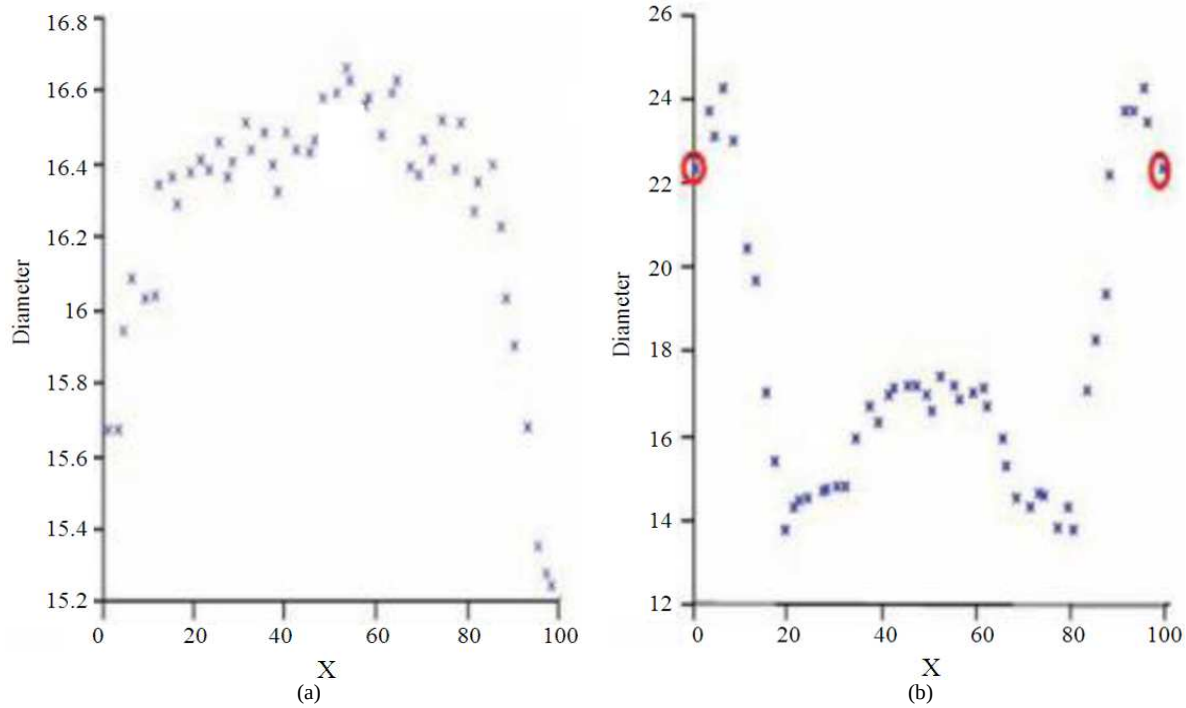


Fig. 7. The diameter with/without a wormhole (a) Network without a wormhole, (b) Network with a wormhole

In the geographic based network layout, a diameter element is used to sense wormholes by identifying bends in local maps; as for the layout built by RTT information, the increase in RTT is take in the consideration. The insight behind these methods is that the wormhole will amplify the number of neighbors of the nodes, shortens the path and increases the real RTT value between successive nodes. **Figure 7** shows the difference of diameter with/without a wormhole.

5. CONCLUSION

In this study, we consider the problem of wormhole attacks in ad-hoc networks. We discussed and compared the state of art wormhole defense approaches and categorized them. In order to formalize the comparison of the discussed wormhole defense methods, we considered the following standards characteristics: localized and distributed specific hardware and software requirements, wormhole detection and isolation, suitability for static and dynamic network, delay cost and detection granulate. In future work we will discuss some more sophisticated wormholes using Mobile agents.

6. REFERENCES

Arora, M., R. Challa and D. Bansal, 2010. Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks. Proceedings of the Second International Conference on Computer and Network Technology, Apr. 23-25, IEEE Xplore Press, Bangkok, pp: 102-104. DOI: 10.1109/ICCNT.2010.34

Bellare, M., R. Canetti and H. Krawczyk, 1996. Keying hash functions for message authentication. Adv. Cryptol., 1109: 1-15. DOI: 10.1007/3-540-68697-5_1

Cressie, N., 1992. Statistics for spatial data. Terra Nova, 4: 613-617. DOI: 10.1111/j.1365-3121.1992.tb00605.x

Du, W., L. Fang and N. Peng, 2006. Lad: Localization anomaly detection for wireless sensor networks. J. Parallel Distrib. Comput., 66: 874-886. DOI: 10.1016/j.jpdc.2005.12.011

Farago, A., 2002. Scalable analysis and design of ad hoc networks via random graph theory. Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Sept. 28-28, ACM Press, Atlanta, GA, USA., pp: 43-50. DOI: 10.1145/570810.570816

Hofmann-Wellenhof, B., H. Lichtenegger and J. Collins, 1993. Global Posi-Tioning System. 1st Edn., Theory Practice.

Hu, Y.C., A. Perrig and D.B. Johnson, 2003. Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of the IEEE Societies 22nd Annual Joint Conference of the IEEE Computer and Communications, Apr. 30-May 3, IEEE Xplore Press, pp: 1976-1986. DOI: 10.1109/INFCOM.2003.1209219

Hu, Y.C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Selected Areas Commun., 24: 370-380. DOI: 10.1109/JSAC.2005.861394

Huang, Y. and W. Lee, 2003. A cooperative intrusion detection system for ad hoc networks. Proceedings of the 1st ACM workshop on Security of Ad Hoc and Sensor Networks, Oct. 27-30, ACM Press, Washington, DC, USA., pp: 135-147. DOI: 10.1145/986858.986877

Jain, M. and H. Kandwal, 2009. A survey on complex wormhole attack in wireless ad hoc networks. Proceedings of the International Conference on Advances in Computing, Control and Telecommunication Technologies, Dec. 28-29, IEEE Xplore Press, Trivandrum, Kerala, pp: 555-558. DOI: 10.1109/ACT.2009.141

Khalil, I., S. Bagchi and N.B Shroff, 2005. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. Proceedings of the International Conference on Dependable Systems and Networks, Jun. 28-Jul. 1, IEEE Xplore Press, pp: 612-621. DOI: 10.1109/DSN.2005.58

Khalil, I., S. Bagchi and N.B. Shroff, 2008. MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Netw., 6: 344-362. DOI: 10.1016/j.adhoc.2007.02.001

Liu, D., P. Ning and W.K. Du, 2005. Attack-resistant location estimation in sensor networks. Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, (IPSN' 05), ACM Press, Piscataway, NJ, USA., pp: 13-13.

Lombardi, M.A., P.L.U. Time and F. Division, 2005. WWVB Radio Controlled Clocks: Recommended Practices for Manufacturers and Consumers. 1st Edn., U.S. Government Printing Office, Washington, DC., ISBN-10: 0160732794, pp: 59.

Maheshwari, R., J. Gao and S.R. Das, 2007. Detecting wormhole attacks in wireless networks using connectivity information. Proceedings of the 26th IEEE International Conference on Computer Communications, May 6-12, IEEE Xplore Press, Anchorage, AK., pp: 107-115. DOI: 10.1109/INFCOM.2007.21

Merkle, R., 1980. Protocols for public key cryptosystems. Proceedings of the IEEE Symposium on Security and Privacy, (SSP' 80), IEEE Computer Society Press, pp: 122-134.

Mills, D.L., 1992. A computer-controlled LORAN-C receiver for precision timekeeping. University of Delaware.

Nasipuri, A., R. Castaneda and S.R. Das, 2001. Performance of multipath routing for on-demand protocols in mobile ad hoc networks. Mobile Netw. Appli., 6: 339-349. DOI: 10.1023/A:1011426611520

Papadimitratos, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, Jan. 27-31, San Antonio, TX, pp: 193-204.

Perrig, A., R. Canetti, J.D. Tygar and D. Song, 2000. Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy, May 14-17, IEEE Xplore Press, Berkeley, CA., pp: 56-73. DOI: 10.1109/SECPRI.2000.848446

Pirzada, A.A. and C. McDonald, 2004. Establishing trust in pure ad-hoc networks. Proceedings of the 27th Australasian Conference on Computer Science, (ACCS' 04), Australian Computer Society, Inc. Darlinghurst, Australia, pp: 47-54.

Poovendran, R. and L. Lazos, 2007. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Netw., 13: 27-59. DOI: 10.1007/s11276-006-3723-x

Prasannajit, B., Venkatesh, S. Anupama, K. Vindhykumari and S. Subhashini *et al*., 2010. An approach towards detection of wormhole attack in sensor networks. Proceedings of the 1st International Conference on Integrated Intelligent Computing, (ICIIC), Aug. 5-7, IEEE Xplore Press, Bangalore, pp: 283-289. DOI: 10.1109/ICIIC.2010.54

Ramaswamy, S., H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, 2003. Prevention of cooperative black hole attack in wireless ad hoc networks. Proceedings of the International Conference on Wireless Networks, (WN' 03), CiteSeerX, pp: 570-575.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E. Belding-Royer, 2002. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols, Nov. 12-15, IEEE Xplore Press, pp: 78-87. DOI: 10.1109/ICNP.2002.1181388

Sen, J., M.G. Chandra, S.G. Harihara, H. Reddy and P. Balamuralidhar, 2007. A mechanism for detection of gray hole attack in mobile Ad Hoc networks. Proceedings of the 6th International Conference on Information, Communications and Signal Processing, Dec. 10-13, IEEE Xplore Press, Singapore, pp: 1-5. DOI: 10.1109/ICICS.2007.4449664

Tamilselvan, L. and V. Sankaranarayanan, 2007. Prevention of impersonation attack in wireless mobile ad hoc networks. Int. J. Comput. Sci. Network Security, 7: 118-118.

Wang, W. and B. Bhargava, 2004. Visualization of wormholes in sensor networks. Proceedings of the 3rd ACM Workshop on Wireless Security, Oct. 01-01, ACM Press, Philadelphia, PA, USA., pp: 51-60. DOI: 10.1145/1023646.1023657

Wang, Y., Z. Zhang and J. Wu, 2010. A distributed approach for hidden wormhole detection with neighborhood information. Proceedings of the 5th International Conference on Networking, Architecture and Storage, (NAS), IEEE Xplore Press, Macau, pp: 63-72. DOI: 10.1109/NAS.2010.22

Xu, Y., J. Ford and F.S. Makedon, 2006. A variation on hop-counting for geographic routing. Proceedings of the IEEE Workshop on Embedded Networked Sensors, (WENS' 06), CiteSeerX.

Zhao, Z., W. Bo, X. Dong, L. Yao and F. Gao, 2010. Detecting wormhole attacks in wireless sensor networks with statistical analysis. Proceedings of the International Conference on Information Engineering (ICIE), Aug. 14-15, IEEE Xplore Press, Beidaihe, Hebei, pp: 251-254. DOI: 10.1109/ICIE.2010.66