ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS

Viren Mahajan, Maitreya Natu, and Adarshpal Sethi
University of Delaware
{mahajan,natu,sethi}@cis.udel.edu

ABSTRACT [*]

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another. Our focus in this paper is a particular form of the wormhole attack called the self-contained in-band wormhole. In this paper we analyze the criterion for successful wormhole attack on a MANET. Based on results collected from a Qualnet simulation, we evaluate the likelihood of such an attack. We further classify the wormhole scenarios into successful, unsuccessful, doubtful, interesting, and uninteresting. We also define wormhole strength and observe that the detection ratio of the technique proposed in [12] varies with wormhole strength as well as with the network topology. The simulation statistics also show that the wormholes having higher strength have a higher detection ratio as compared to the ones with lower strength.

1. INTRODUCTION

A *wormhole* is an attack on the routing protocol of a Mobile Ad-hoc Network (MANET). In a wormhole attack, two or more colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another. This shortcut is created by connecting the purported neighbors through a covert communication channel. A wormhole thus allows an attacker to create two attacker-controlled choke points which can be utilized by the attacker to degrade or analyze traffic at a desired time. Our focus in this paper is a particular form of the wormhole attack called the self-contained in-band wormhole.

Many intrusions hold a close resemblance to faults in their manifestation. A case for integrated intrusion detection and fault localization was made in [14]. In continuation of that work, an intrusion detection system to detect wormhole using fault localization techniques was proposed in [12]. It exploited anomaly in the end-to-end delay and per-hop delay patterns to identify the nodes involved in a wormhole attack and gave an architecture and an algorithm for wormhole detection.

In this paper we analyze the criterion for successful wormhole attack on a MANET. We have collected some simulation statistics and based upon them we evaluate the probability of such an attack. We further classify the wormhole scenarios into successful, unsuccessful, doubtful, interesting, and uninteresting. We also define wormhole strength and observe that the detection ratio of the technique proposed in [12] varies with wormhole strength as well as with the network topology. The simulation statistics also show that the wormholes having higher strength have a higher detection ratio as compared to the ones with lower strength.

This paper is organized as follows: Section 2 presents the related work. Section 3 describes the wormhole attack and its different variations. Section 4 presents a number of metrics to compute the strength of a wormhole and presents analysis of the strength of different wormholes in a network. Section 5 describes various ways in which a wormhole attack manifests itself in a network through abnormal patterns of delay, loss, and hop-count distribution, which can be used as the basis for a defense mechanism to detect a wormhole in the network. Section 6 presents the results of a simulation study that shows the likelihood of wormhole attacks and their strengths. Section 7 presents the summary and conclusion.

2. RELATED WORK

Past research has examined the problem of detecting out-of-band wormhole attacks. Hu *et al* [8] described the out-of-band wormhole concept and presented several countermeasures to detect remote forwarding of packets. Hafslund *et al* [6] and Hong *et al* [7] defined security extensions to OLSR to prevent generation of false OLSR messages or replay of legitimate OLSR messages. Lazos *et al* [10] proposed a geography-based countermeasure to defend the wormhole attack. Some of these methods propose to defend by temporally or geographically limiting the spread of HELLO messages. However, a self-contained

[*] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

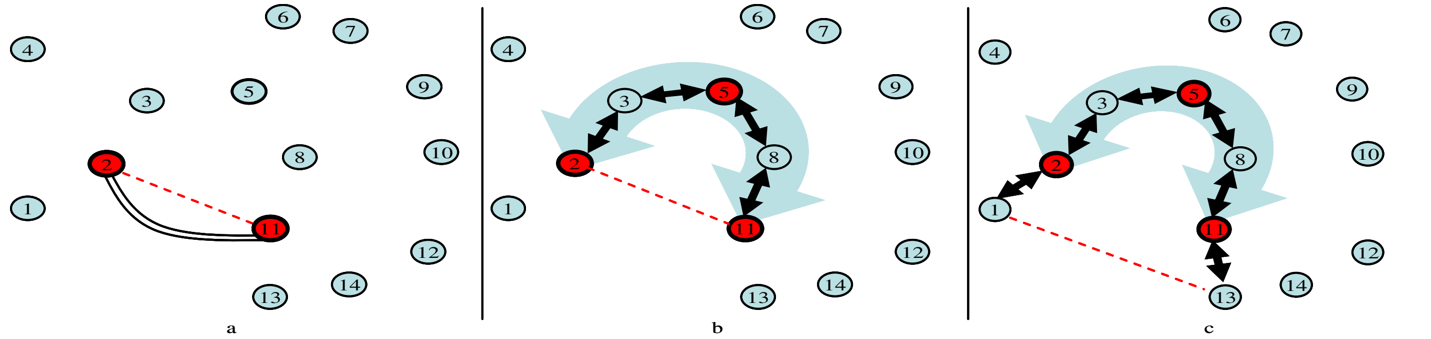

Figure 1: (a) Out-of-band wormhole using an external wired link between attacker nodes 2 and 11, (b) Self-contained in-band wormhole between nodes 2 and 11 using an overlay tunnel passing through another colluder node 5, (c) Extended in-band wormhole by creating false link between nodes 1 and 13 by attacker nodes 2, 11, and 5.

in-band wormhole attack does not require exchange of HELLO messages and can defeat such defenses. Also some approaches rely on using source authentication using signing keys. Such defenses can be defeated if a node is compromised and the attacker has access to secured information. Baras et al [1] proposed a mechanism to detect a self-contained in-band wormhole by observing the anomaly between the cumulative path loss and delay and the perceived path length. Cardenas et al [3] proposed an approach based on the space-time framework to detect the changed hop count distribution caused by a wormhole. These approaches detect the wormhole endpoints. They cannot identify the intermediate tunnel nodes that knowingly or unknowingly participate in forming a wormhole tunnel. Kruus et al [9] proposed several countermeasures for wormhole detection and prevention. These countermeasures include 1) OLSR protocol extensions that incorporate link quality in routing decisions, 2) higher protocol layer measurements of packet loss and round-trip delays over 1-hop and 3-hop routing paths, and 3) monitoring for the presence of asymmetric links and other potential indicators. Awerbuch et al [15] propose using encryption and packet loss for identifying bad links in the network.

3. WORMHOLE ATTACK PHENOMENON

In this section, we present different variations of a wormhole attack.

3.1 In-band and out-of-band wormholes

In an out-of-band wormhole, the colluder nodes establish a direct link between the two end-points of the wormhole tunnel in the network. This link is established using a wired link or a long-range wireless transmission. Figure 1a shows an out-of-band wormhole established in a network by two colluding nodes. The wormhole attacker then receives packets at one end and directs the packets to be forwarded to the other end through the established link. The attacker can thus analyze and tamper a large amount of traffic through this link.

An in-band wormhole, on the other hand, does not use an external communication medium to develop the link between the colluding nodes. An in-band wormhole instead develops a covert overlay tunnel over the existing wireless medium. An in-band wormhole can be a preferred choice of attackers and can be potentially more harmful as it does not require any additional hardware infrastructure and consumes existing communication medium capacity for routing the tunneled traffic. Figure 1b shows an in-band wormhole developed over a wireless network using false OLSR messages. Nodes 2 and 11 create an illusion of being neighbors by sending false routing advertisements of a 1-hop symmetric link between the two nodes without the actual exchange of HELLO messages. This false link information is propagated to other nodes across the network via a broadcast of OLSR Topology Control (TC) messages. This false link information thus undermines the shortest path routing calculations attracting many end-to-end flows by advertising incorrect shortest paths. The attracted traffic is then forwarded through a tunnel with the help of a third colluder node, node 5. This colluder node acts as an application-layer relay for wormhole traffic between the wormhole endpoints.

3.2 Self-contained and extended in-band wormholes

We now describe two forms of in-band wormholes: extended in-band wormhole and self-contained in-band wormhole. An extended wormhole creates a wormhole that extends beyond the attackers forming the tunnel endpoints. A false link is advertised between two nodes that are not the attacker nodes. A potentially stealthier self-contained wormhole, on the other hand, advertises a false link between the attacker nodes themselves.

Figure 1c presents an example of an extended wormhole. The attacker nodes 2 and 11 forming the tunnel endpoints capture HELLO messages from nodes 1 and 13 and forward them through the relay node 5 to pass through the tunnel to the other end. All subsequent OLSR control and data messages are forwarded in a similar fashion. This results in a false link between nodes 1 and 13 extending the wormhole beyond the endpoint nodes 2 and 11.

Figure 1b presents an example of a self-contained wormhole, where the attacker nodes 2 and 11, forward their own HELLO messages to each other, or simply falsely report each other as neighbors by sending incorrect HELLO messages. The incorrect HELLO messages, further broadcast by TC messages, lead to advertisement of a false link between the two attacker nodes 2 and 11, developing a self-contained in-band wormhole.

4. WORMHOLE ATTACK ANALYSIS

4.1 Placement of wormhole colluder nodes:

The placement of compromised nodes to launch a wormhole attack plays an important role in the effectiveness of a wormhole. Below we present some scenarios where a wormhole attack cannot be launched or cannot persist. We present scenarios where three colluder nodes launch a self-contained in-band wormhole attack. In this paper, we assume that the attacker has the ability to bypass the routing algorithm at all three attacking nodes.

Consider the scenario depicted in Figure 2 where nodes 2, 9, and 12 are the attacker nodes. Nodes 2 and 12 act as the wormhole tunnel endpoints and node 9 is the relay node. Nodes 2 and 12 attract network traffic by sending false advertisement of being neighbors and attempt to send the attracted traffic between one another via the relay node 9. The traffic passing from node 2 to node 12 first passes through nodes 3, 4, 5, 6, and 7 to node 9, and then through node 10 to node 12. Nodes 3, 4, 5, 6, 7, and 10 are uncompromised nodes and thus are misled by the incorrect routing advertisement of the link between nodes 2 and 12. When node 3 receives a packet from node 2 to be destined for node 9, node 3 finds the shortest path to node 9 via the link between nodes 2 and 12, and thus forwards the packet back to node 2, making the wormhole attack fall victim to its own success.

The wormhole tunnel cannot be formed successfully in the scenario shown in Figure 2 because the path from node 3 to node 9 via nodes 4, 5, 6, and 7 is of length 5 hops. On the other hand, the path from node 3 to node 9 via the wormhole link purports to pass through the sequence of nodes 2, 12, 10, and 9, thus advertising a shorter path length of 4 hops.

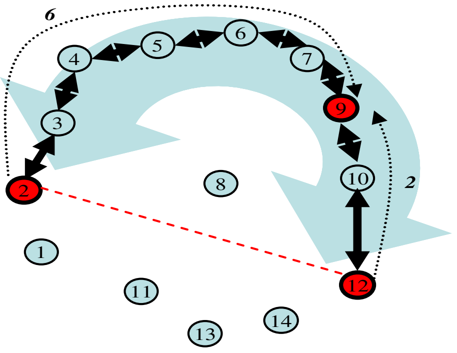

Figure 2: A scenario where wormhole tunneling fails as node 3 finds a shorter path to reach node 9 via the wormhole link.

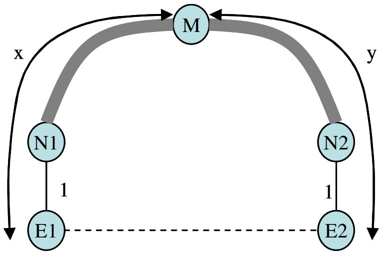

Figure 3: Figure representing the wormhole constructed by attacker nodes E1 and E2. Figure shows the paths of length x and y from E1 and E2 respectively to the intermediate attacker node M. Nodes N1 and N2 lie on the paths from E1 and E2 to M respectively.

Let E1 and E2 represent the tunnel end points and node M represent the intermediate relay node as shown in Figure 3. Let N1 and N2 be the first uncompromised nodes on the paths from E1 and E2 to M respectively that do not pass through the wormhole link. Let the path from E1 to M that does not pass through the wormhole link be of length *x* hops, and that from E2 to M be of length *y* hops. To prevent nodes N1 and N2 from getting attracted to the wormhole link to route traffic to node M, the length of the paths from N1 and N2 to M should be less than that offered by the path passing through the wormhole link. The length of the path from N1 to M via the wormhole link is *y+2* hops. Thus the actual path from N1 to M should be less than *y+2* hops. As N1 is a neighbor of E1, the length of the path from E1 to M should be less than *y+3* hops. Thus,

$$x < y + 3 \tag{1}$$

The path from N2 to M is *y-1* hops. To prevent N2 from getting attracted by the wormhole link E1-E2, the path from N2 to M offered by the wormhole link should be greater than *y-1* hops. The path from N2 to M passing through the wormhole link is of length *x+2* hops. Thus,

$$x + 2 > y - 1 \tag{2}$$

From equations 1 and 2, it then follows that:

$$y - 3 < x < y + 3 \tag{3}$$

So we see that only those three node combinations can be used to create a wormhole where *x* lies between *y* – 3 and *y* + 3. But even in such scenarios, it is possible that the wormhole does not get created successfully. Consider the example in Figure 4 where nodes 1 and 7 act as the tunnel end points while node 5 is the tunnel mid node. When the end node 7 tries to send a packet to the end node 1, the packet will be encapsulated by the tunnel and sent to the middle node 5. Since the middle node 5 is capable of bypassing the routing protocol, it will correctly forward the packet to the next hop i.e. node 4. Since the node 4 is not capable of bypassing the routing protocol, it will find the shortest path to node 1 via the link between the nodes 7 and 1, and so node 4 will forward the packet back to node 7. So again the wormhole attack will fall victim to its own success. Further, we can also see that as the difference between x and y increases, the chances of such a situation arising and leading to wormhole collapse increase.

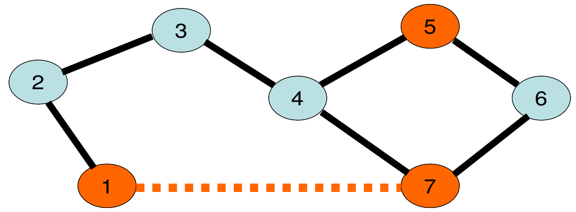

Figure 4: A scenario showing the problem of wormhole collapse due to the presence of link between a non-attacker node lying on the wormhole tunnel and a wormhole end node.

From the above analysis, it is clear that not all three-node combinations of attacker nodes can be used to create a wormhole. We thus classify all the three-node combinations that can be formed out of all the nodes present in a network into the following categories:

- *Successful Wormhole*: These are scenarios where we are most hopeful that a successful wormhole can be created. We propose that the combinations satisfying the following criteria should be classified as successful: $y - 2 < x < y + 2$
- *Unsuccessful Wormhole:* We expect the scenarios where x is less than or equal to y-3 or x is greater than or equal to y+3 to be unsuccessful in the creation of a wormhole.
- *Doubtful Wormhole:* The three-node combinations that are on the boundary line between successful and unsuccessful are regarded as doubtful. These are the scenarios in which x is equal to y+2 or y-2 hops.

Figure 5 depicts examples of various such wormhole scenarios according to the above classification. Figures 5a and 5b present the *Successful Wormhole* scenarios. In Figure 5c, although the path from node N to node M through the wormhole link is longer, but the wormhole could still fail for reason shown in Figure 4. This is an example of *Doubtful Wormhole* scenario. Figure 5d shows the case when the path from E1 to M is of length y+3 hops. Here node N has two paths to node M which are of length y+2. The wormhole tunneling will succeed only if the path not passing through the link E1-E2 is chosen to route traffic from node N to node M. In any case, even if a wormhole does get created, it may not be sustainable if the routing table entries change. Apart from this, there are chances of the wormhole failing for reason shown in Figure 4. Figure 5e presents a case where the wormhole tunneling fails as the wormhole link E1-E2 provides a shorter path from node N to M. Both the above cases are considered as *Unsuccessful Wormhole* scenarios.

Further, if the nodes that are chosen to form wormhole end points are actually one-hop neighbors, they will not attract any extra traffic. So they might not appear interesting to the attacker whose purpose is to attract more traffic into the tunnel. This gives us another criterion for classifying the node combinations and we apply this criterion to further classify the *Successful* combination of nodes into the following two sub-categories:

- *Successful Interesting*: The Successful node combinations where the nodes chosen for being the wormhole end-points are not actually one-hop neighbors.
- *Successful Uninteresting*: The Successful node combinations where the nodes chosen for being the wormhole end-points are actually one-hop neighbors.

4.2 Metrics for a wormhole attack

1. Strength: The effectiveness of a wormhole attack is based on the amount of traffic that can be attracted by a wormhole. The larger the amount of attracted traffic, stronger can be the wormhole attack on the network traffic. We define the *strength* of a wormhole attack as the number of end-to-end paths attracted by the false link advertisement sent by the attackers. In other words, the strength of a wormhole is the number of end-to-end paths passing through the wormhole tunnel.

2. Difference between the advertised and actual path length: Another metric for a wormhole attack is the difference in the advertised path length and the actual path length. For instance, in Figure 1b the advertised path from 1 to 13 passes through the nodes 1, 2, 11, and 13, advertising a path length of 3 hops. However, the actual path from 1 to 13 passes through the nodes 1, 2, 3, 5, 8, 11, and 13, making the actual path of length 6 hops. This metric can be useful for the purpose of detection of the wormhole. The larger the difference, the stronger anomalies can be observed in the network.

3. Attraction: This metric refers to the decrease in the path length offered by the wormhole. For instance, in Figure 1b, before the wormhole attack, the path from node 3 to

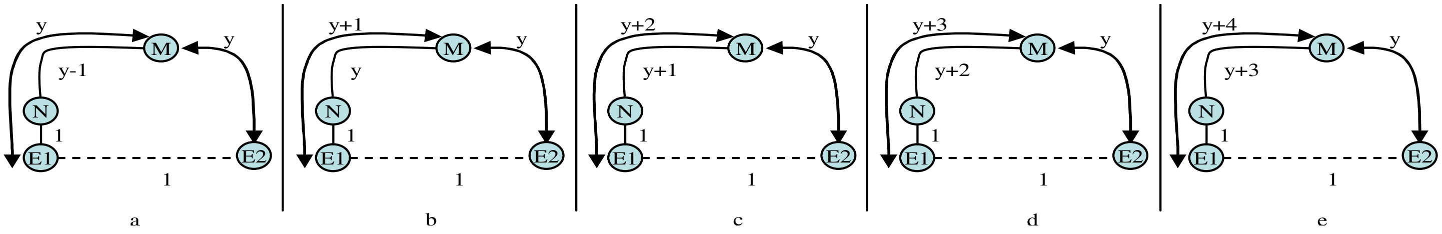

Figure 5: (a,b) Scenario where wormhole tunneling succeeds as node N finds a shorter path to node M that does not pass through the wormhole link, (c,d) Wormhole might collapse due to the presence of link between a non-attacker node lying on the wormhole tunnel and a wormhole end node. Further in (d), the success of wormhole tunneling depends on routing policy of choosing one of the two paths to reach node M, (e) Wormhole tunneling fails as node N finds a shorter path to node M passing through the wormhole link.

node 13 might pass through the nodes 3, 5, 8, 11, and 13. After the wormhole attack, the path passes through the nodes 3, 2, 11, and 13, decreasing the path length by 1 hop.

4. Robustness: Robustness of a wormhole refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network. The resilience of the wormhole to small changes of topology is based on the amount of *attraction* offered by the wormhole. If the *attraction* is small then small improvements in normal paths can result in nodes choosing alternative paths that do not pass through the wormhole link, thus decreasing the *strength* of the wormhole.

5. PROPOSED DEFENSE

A wormhole attack will exhibit certain abnormal network behavior that can be exploited to develop defenses against such attacks. In this section, we present various characteristics that can be observed in a network in the presence of a wormhole attack.

5.1 Path length distribution

The advertisement of the false wormhole link changes the routes of various end-to-end paths attracted by the wormhole, decreasing the end-to-end path length of all such paths. The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack. Furthermore, the amount of decrease in the path lengths would then be based on the *attraction* of the wormhole.

5.2 Delay

The delay statistics can generate following anomalies on the launch of a wormhole attack.

5.2.1 Incompatible hop delays and end-to-end delay: The paths that are attracted by a wormhole have different advertised and actual routes. The advertised routes in this case are much shorter than the actual routes which go through the wormhole tunnel. For instance, consider the path between nodes 1 and 12 in Figure 6. The advertised route for this path goes through nodes 1, 2, 11, and 12, but the actual route taken by packets between nodes 1 and 12 goes through nodes 1, 2, 3, 5, 8, 11, and 12. A large part of the end-to-end delay for a path consists of hop delays at each hop. Thus, with the available advertised path information, the end-to-end delay for such a path will not be explained by the sum of hop delays of the hops present on its advertised path.

5.2.2 Increased end-to-end delay: Another anomaly can be observed on the nodes that form the wormhole tunnel. The traffic received by these nodes is not explained by the overall end-to-end traffic. Given the advertised routes and the amount of end-to-end traffic, the amount of traffic received by these nodes should be significantly less than what the nodes actually receive. The additional unexplained traffic is due to the wormhole tunnel traffic. Thus due to the wormhole, the hop delay of tunnel nodes would increase. This in turn would increase the end-to-end delay of the routes that do not get attracted by the wormhole but pass through some of the tunnel nodes. For instance, in Figure 6, the path between nodes 4 and 6 does not get attracted by the wormhole but actually goes through nodes 3 and 5 that are part of the wormhole tunnel. Nodes 3 and 5 would have increased hop delay due to the wormhole traffic, leading to an increased end-to-end delay on the path between nodes 4 and 6. Thus, unlike the previous anomaly, paths belonging to this anomaly show a consistent end-to-end delay and hop delay sum. However, they show an abrupt increase in the end-to-end delay and the hop queuing delay values that are not explained by the traffic supposedly flowing through these nodes.

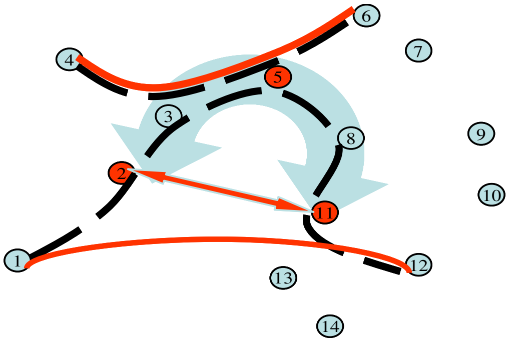

Figure 6: Network topology with wormhole created by nodes 2, 5, and 11. Figure shows actual paths with dashed lines and advertised paths with solid lines. Actual path between nodes 1 and 12 is different from advertised path. Actual path and the advertised path between nodes 4 and 6 stay the same, but overlap with the wormhole tunnel.

6. SIMULATION RESULTS

We have conducted simulations of wormhole attacks in an ad-hoc network using OLSR. The simulations were designed in the Qualnet simulation platform. The network size was 1000*1000 meters. We ran the simulations with multiple topologies having 15, 25 and 50 nodes. These topologies were generated in a pseudo-random manner. For each network topology, we identified some sets of nodes which could be made the wormhole endpoints (as explained below). Then we ran multiple simulations on that topology changing the combination of wormhole nodes each time.

6.1 Feasibility of Wormhole Attack

One of the objectives of the simulation was to examine the feasibility of a wormhole attack. Given a configuration of nodes in an ad-hoc network, what is the likelihood that an attacker who compromises three random nodes in the network can create a viable wormhole? As explained in Section 4.1, not all three-node combinations can be used to

Table 1: Number of node combinations of each type with different node topologies

No. of Nodes	Total Combinations	Wormhole Create Failure	Successful Wormhole Combinations			Doubtful Wormhole Combinations		Unsuccessful Wormhole Combinations	
			Interesting	Result %	Uninteresting	Total	Result %	Total	Result %
15	1365	186	675	98	350	147	61	7	28
15	1365	196	643	97	345	173	62	8	12
15	1365	177	627	97	397	164	65	0	0
25	6900	602	3442	97	1794	955	67	107	42
25	6900	720	3219	93	1498	1266	70	197	42
25	6900	686	3379	98	1563	1069	69	203	44
50	58800	1867	27584	79	23545	5443	47	361	36
50	58800	2081	29041	85	20705	6575	51	398	42
50	58800	2382	29291	71	18016	8494	39	617	41

Table 2: Showing the comparison of strength with detection ratio for four different topologies

Topology	Strength	Detection Ratio (%)
1	High (>=14)	100.00
	Medium (6-13)	78.43
	Low (<=5)	34.43
2	High (>=14)	88.68
	Medium (6-13)	76.79
	Low (<=5)	40.00
3	High (>=14)	75.00
	Medium (6-13)	76.31
	Low (<=5)	70.00
4	High (>=14)	21.05
	Medium (6-13)	49.35
	Low (<=5)	41.49

create a wormhole, and we had classified all the three-node combinations that can be formed out of all the nodes that are present in a network as *Successful*, *Unsuccessful* and *Doubtful*. The Successful combinations were further divided into *Successful Interesting* and *Successful Uninteresting*.

In our simulations, we counted the actual numbers that correspond to these categories of three-node combinations in a network. We applied the above criteria to multiple topologies generated in a random/pseudo-random manner and came up with the results shown in Table 1. As can be seen from the first row of the table, for a fifteen node topology there are 1365 different three-node combinations out of which 675 fall under the *Successful Interesting* category. Although 675 is quite a small percentage of the total three-node combinations available, but it is quite a large number in itself. Further, for each network topology and type of wormhole node combination, we ran 100 simulations to actually see in how many cases the wormhole persists successfully. As per our belief, in each of the cases the wormholes generated from *Successful Wormhole* category have a higher chance of persistence as compared to those generated from the *Doubtful Wormhole* and *Unsuccessful Wormhole* categories. Again looking at the first row of Table 1, we can see that in 98 percent of the *Successful Interesting* cases the wormhole persisted successfully while wormhole persisted successfully in only 61 percent of the *Doubtful Wormhole* cases. Further there were only seven cases of unsuccessful wormhole found in this topology out of which only two persisted successfully. Similarly the other rows of the table show quite a large number of three-node combinations falling under the *Successful Interesting* category. This leads us to believe that the wormhole attack is quite a feasible phenomenon with many options available to the attacker.

6.2 Effect of strength on DR

Presently we are using the delays as the criterion for identifying the wormhole. The DR is expected to increase with the strength of wormhole. This is because more number of paths getting attracted towards the wormhole will result in more traffic passing through the wormhole tunnel nodes. This will further increase the hop delay experienced by packets at these tunnel nodes. Thus the delay criterion that we use for detecting the wormhole will become more pronounced in this case. Specifically this has the following effect on each of the delay criteria:

6.2.1 Incompatible hop delays and end-to-end delay: For the packets that are passing through the wormhole tunnel, the end-to-end delay would further increase as the hop delay experienced at each tunnel node increases. The sum of hop delays however remains the same. Thus the difference between the actual and the perceived delay would further increase indicating the presence of a wormhole.

6.2.2 Increased end-to-end delay: Similarly for the nodes that form the wormhole tunnel, there is a further increase in the additional unexplained traffic that passes through these nodes. Due to the increase in the hop delays at these nodes, the paths that do not get attracted by wormhole but pass through some of the tunnel nodes will experience an increase in end-to-end delay. With the increase in the strength of the wormhole, this increase will become more abrupt and help in the detection of the wormhole tunnel nodes.

For 15 node topologies on a network size of 1500*1500 meters, we classified the successful wormholes into high, medium and low strength wormholes as follows:

- *High Strength:* number of paths passing through the wormhole >= 14
- *Medium strength*: number of paths passing through the wormhole between 6 & 13

- *Low strength*: number of paths passing through the wormhole <= 5

The results of our simulation experiments correlating Detection Ratio with wormhole strength are shown in Table 2. These simulations were performed on a network size of 1500*1500 meters with 15 node random/pseudo-random topologies. As seen from this table, the simulation results are in line with our hypothesis. Generally, the wormholes with high strength show a higher detection ratio as compared to the wormholes with lower strength as seen with topologies 1 and 2. However in some cases, the results are not in sync with the general hypothesis (topology 4). This can be attributed to the clustering of nodes in the network. We are currently examining this phenomenon and will conduct more simulations to analyze it further.

7. CONCLUSIONS AND FUTURE WORK

In this paper we have explained the self-contained in-band wormhole phenomenon and identified the conditions that are necessary for the such an attack to persist. We have classified all the possible three-node combinations in a network accordingly. We have also given some metrics to judge a wormhole attack and explained how those metrics help with the strategy that we use for the detection of such an attack. Finally we have presented the simulation results and shown the number of possibilities available with the attacker for some scenarios. As part of the future work, we plan to use packet loss as a criteria for the detection of wormhole along with the current method in order to improve the detection ratio.

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

REFERENCES

[1] J.S. Baras, A.A. Cardenas, and V. Ramezani, "On-line detection of distributed attacks from space-time network flow patterns." In ASC'04, the 24th Army Science Conference, Orlando, FL, Nov. 2004.

[2] M. Brodie, I. Rish, and S. Ma, "Optimizing probe selection for fault localization." In DSOM-2001, IFIP/IEEE International Workshop on Distributed Systems Operations and Management, Nancy, France, Oct. 2001.

[3] A.A. Cardenas, J.S. Baras, and V. Ramezani, "Distributed change detection for worms, DDoS and other network attacks." In ASC'03, the 23rd Army Science Conference, 2003.

[4] R. Gopaul, P. Kruus, D. Sterne, and B. Rivera, "Gravitational analysis of the in-band wormhole phenomenon", Proc. 25th Army Science Conference, Orlando, FL, Nov. 2007.

[5] M. Gorlatova, P. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting wormhole attacks in mobile ad-hoc networks through protocol breaking and packet timing analysis." In MILCOM 2006, Washington, DC, Oct. 2006.

[6] A. Hafslund, A. Tonnesen, R. Bjorgum Rotvik, J. Anderson, and O. Kure, "Secure extensions to the OLSR protocol." In OLSR Interop Workshop, San Diego, Aug. 2004.

[7] F. Hong, L. Hong, and C. Fu, "Secure OLSR." In 19th International Conference on Advanced Information Networking and Applications (AINA'05), volume 1, pages 713–718, 2005.

[8] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks." In IEEE Infocom, 2003.

[9] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, and N. Ivanic, "In-band wormholes and countermeasures in OLSR networks." In SecureComm2006, Baltimore, MD, Aug. 2006.

[10] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L.W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach." In IEEE Wireless Communications and Networking Conference (WCNC), 2005.

[11] M. Natu and A.S. Sethi, "Adaptive fault localization in mobile ad-hoc battlefield networks." In MILCOM'05, Atlantic City, NJ, 2005.

[12] M. Natu and A.S. Sethi, "Intrusion detection system to detect wormhole using fault localization techniques." In WORLDCOMP SAM'07, International Conference on Security and Management, Las Vegas, NV, June 2007.

[13] M. Steinder and A.S. Sethi, "Probabilistic fault diagnosis in communication systems through incremental hypothesis updating." *Computer Networks*, 45(4):537–562, July 2004.

[14] D. Sterne, S. Tsang, M. Natu, D. Balenson, P. Mouchtaris, and A.S. Sethi, "Integrating intrusion detection and fault localization in MANETs." In Milcom-2006, IEEE Military Communications Conference, Washington, DC, Oct. 2006.

[15] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens, "An on-demand secure routing protocol resilient to byzantine failure." In ACM Workshop on Wireless Security (WiSe), September 2002.