GRAVITATIONAL ANALYSIS OF THE IN-BAND WORMHOLE PHENOMENON

Richard Gopaul[1], Peter Kruus[2], Dan Sterne[2], Brian Rivera[1]

[1]U.S. Army Research Laboratory
Adelphi, MD, 20783 USA

[2]SPARTA, Inc.
Columbia, MD, 21046 USA

ABSTRACT

In-band wormhole attacks undermine routing by attracting network traffic that otherwise may have bypassed the attackers via alternate, lower-cost routes. The result gives the attackers control over the attracted traffic, allowing them to modify, delay, redirect, eavesdrop, or drop the traffic. In this paper we expand upon the *gravitational analysis* technique, first presented in [KSG06], for evaluating the effects of in-band wormhole attacks on OLSR routing. The gravitational analysis technique examines individual network topologies and results in the creation of a "gravitational chart" for each topology. The gravitational charts contain the necessary data to define the attractiveness of a specific wormhole configuration and the penalty incurred by source-destination pairs affected by the wormhole path. We attempt to gain insight into both node and topology vulnerability to the in-band wormhole attack by analyzing the raw data contained within the gravitational charts using several new cost, attraction, and detection metrics defined in this paper. Analysis of the gravitational charts with respect to these metrics allows both topologies and the individual nodes and paths within a topology to be quickly compared and ranked. We can then easily identify those topologies that are most or least impacted by the wormhole and assess the specific topological characteristics responsible, facilitating more efficient and effective intrusion detection system design.

1. INTRODUCTION

Future Combat Systems will rely heavily on mobile, survivable computer networks to achieve dominance on the battlefield. In particular, mobile ad-hoc network (MANET) technologies are likely to play a key role as the Army migrates toward Network Centric Warfare. Current MANET routing protocols, however, lack the security necessary to operate in a tactical environment and are vulnerable to many forms of attack [HU03][ADJ05]. Of particular interest is the *in-band wormhole* attack, in which compromised nodes collude to create the illusion that distant regions of a MANET are directly connected [KSG06]. The attack undermines MANET routing and attracts network traffic that otherwise may have bypassed the attackers via alternate, lower-cost routes. Also, because the attack tunnels traffic in a suboptimal manner within the MANET itself, in-band wormholes continually consume network capacity (i.e., waste bandwidth). This can cause congestion at the wormhole choke points which could lead to an overall service degradation.

In the attack, colluding attackers covertly connect the purported neighbors via multi-hop tunnels established through the same routing infrastructure under attack. The result gives the attackers control over the attracted traffic, allowing them to modify, delay, redirect, eavesdrop, or drop the traffic. Also, because the attack uses the existing routing resources, it continually consumes network capacity, inherently degrading service.

[KSG06] introduces a new analytical technique for evaluating the affects of wormhole attacks on a routing topology called g*ravitational analysis*. Gravitational analysis examines individual network topologies with a specific wormhole configuration and results in the creation of a "gravitational chart" for each topology which contains the necessary data to define the attractiveness of the wormhole and the penalty incurred by source-destination pairs affected by the wormhole path.

This paper expands upon the basic gravitational analysis techniques by defining several new metrics that more broadly measure the impact of an in-band wormhole attack on a Optimized Link State Routing (OLSR) MANET topology [OLSR03]. Rather than focusing solely on specific source-destination paths within a topology, these new metrics measure the overall impact of the attack on individual nodes as well as the broader effects on a specific topology. Consequently, the new metrics foster direct comparisons of node placement within a topology as well as inter-topology comparisons, allowing for a better understanding of the attack and its impact on routing. Using these quantitative measurements of wormhole presence within a MANET, we are better able to understand the phenomenon and make tradeoffs between detection and protection mechanisms, facilitating more efficient and effective intrusion detection system design.

This paper is organized as follows. Section 2 provides background matter on both the in-band wormhole attack and the gravitational analysis technique. Section 3 defines new metrics to measure the effects of an in-band wormhole on specific nodes in a topology as well as the cumulative effects on the overall topology. Section 4 describes the application of these metrics in a nineteen-node emulated MANET. We then present our conclusions and ideas for future work in the area.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 NOV 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Gravitational Analysis Of The In-Band Wormhole Phenomenon	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory Adelphi, MD, 20783 USA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002075.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**8**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

2. BACKGROUND

In this paper, our primary focus is to examine the effects of *self-contained in-band wormholes* both on individual nodes within a topology and on the topology as a whole. Specifically, we analyze the effects of self-contained in-band wormholes that use *three colluders* as described in [KSG06]. Within an OLSR based MANET, the wormhole-end attackers modify or forward their own HELLO and Topology Control (TC) messages to create the illusion that they are 1-hop neighbors. To other nodes in the network, the fictitious link between the wormhole-end attackers appears as a shortcut between potentially distant network segments. The attackers subsequently attract traffic that may have otherwise bypassed them and must tunnel it, through the MANET, to the far wormhole-end to maintain the facade. In order to avoid what is known as *wormhole collapse*, the wormhole-end attackers enlist the aid of a third, middle-colluder, located equidistant between the wormhole-end attackers. This third colluder serves as an application layer relay point to forward tunneled traffic between the wormhole-end attackers.

The gravitational charts used in in-band wormhole analysis record several metrics related to the attack against a specific topology. For each routing pair that is affected by the wormhole, the chart records the triple *{A, B, C}* where *A i*dentifies the normal hop-count if the in-band wormhole is not present followed by the perceived hop-count with the wormhole, *B*. The metric *C* is the actual hop-count with a persistent wormhole in operation. C's measurement includes the distance to and from the wormhole endpoints as well as the distance traveled through the wormhole tunnel.

Table 1 below presents an example gravitational chart resulting from the gravitational analysis of the self-contained in-band wormhole attack against the 19-node OLSR network depicted in Figure 1. All true one-hop paths between nodes are shown using thin lines, while a heavier line shows the perceived path created by the self-contained in-band wormhole between the attacker nodes 180 and 183. An intermediate colluder, node 185, supports the wormhole tunnel traffic by helping to prevent wormhole collapse. The table records the effects of the wormhole using the triple {A, B, C} for each source-destination pair. For example, the path from 175 to 186 is {5, 3, 8}, showing a normal non-wormhole hop-count of 5, a perceived hop-count of 3 in the presence of a self-contained in-band wormhole, and an actual hop-count of 8 due to the wormhole tunneling.

Using these simple gravitational metrics, we can derive several other useful metrics defined in [KSG06]. The wormhole *cost* on a selected path (in terms of additional hops) is the difference between the actual hop-count with a wormhole and the normal hop-count without a wormhole, *C-A*, and is a measure of the penalty imposed by the wormhole. The *strength of attraction* is the difference between the normal non-wormhole hop-cont and the perceived hop-count with a wormhole, *A-B*. It measures of the resiliency of the wormhole to small changes in the topology that might improve the non-wormhole path length over the wormhole path length. The *potential detectability* of the wormhole along this path is the difference between the actual hop-count and the perceived hop-count, *C-B*. A large disparity between these two values is an indicator of a path's potential to detect an in-band wormhole by measuring, delay, loss or other path characteristics [KSG06].

As an example of gravitational analysis, we examine the results recorded in Table 1 which is calculated for Figure 1. In the table, we see that the triple for the path from node 175 to node 186 is {5, 3, 8}. The normal path cost (A) is 5 measured across the path (191, 189, 197, 184, 186); the perceived path cost (B) is 3 measured along the path (180, 183, 186); the actual wormhole path cost (C) is 8 measured through the longer wormhole tunnel path (180, 191, 189, 185, 197, 184, 183, 186). Applying the derived metrics to these basic metrics, we see that the *cost* for the path between 175 to 186 is 3, the *strength of attraction* is 2, and the *potential detectability* is 5.

Table 1 – Gravitational Chart for the 19-node OLSR Topology in Figure 1

Destination Node

Source Node	175	178	179	180	181	182	183	184	185	186	187	188	189	191	192	196	197	198	199
175	0	2	05/03/08	1	06/03/08	1	05/02/07	04/03/08	3	05/03/08	05/03/08	3	2	1	4	1	3	4	04/04/09
178	2	0	04/04/09	2	05/04/09	3	04/03/08	3	2	04/04/09	04/04/09	2	1	1	3	1	2	3	3
179	05/03/08	04/04/09	0	05/02/07	1	06/03/08	1	1	3	1	1	4	3	04/03/08	3	05/03/08	2	3	2
181	06/03/08	05/04/09	1	06/02/07	0	07/03/08	1	2	4	2	1	5	4	05/03/08	4	06/03/08	3	04/04/04	3
182	1	3	06/03/08	1	07/03/08	0	06/02/07	05/03/08	4	06/03/08	06/03/08	4	3	2	05/05/10	2	4	05/05/10	05/04/09
184	04/03/08	3	1	04/02/07	2	05/03/08	1	0	2	1	1	3	2	03/03/08	2	04/03/08	1	2	1
186	05/03/08	4	1	05/02/07	2	06/03/08	1	1	3	0	1	3	3	04/03/08	2	05/03/08	2	2	1
187	05/03/08	04/04/09	1	05/02/07	1	06/03/08	1	1	3	1	0	4	3	04/03/08	3	05/03/08	2	3	2
188	3	2	4	3	5	4	4	3	1	3	4	0	1	2	1	3	2	1	2
189	2	1	3	2	4	3	03/03/08	2	1	3	3	1	0	1	2	2	1	2	2
191	1	1	04/03/08	1	05/03/08	2	04/02/07	3	2	04/03/08	04/03/08	2	1	0	3	1	2	3	3
192	4	3	3	4	4	5	3	2	1	2	3	1	2	3	0	4	1	1	1
196	1	1	05/03/08	1	06/03/08	2	05/02/07	04/03/08	3	05/03/08	05/03/08	3	2	1	4	0	3	4	4
197	3	2	2	3	3	4	2	1	1	2	2	2	1	2	1	3	0	1	1
198	4	3	3	4	4	5	3	2	1	2	3	1	2	3	1	4	1	0	1
199	4	3	2	04/03/08	3	05/04/09	2	1	2	1	2	2	2	3	1	4	1	1	0

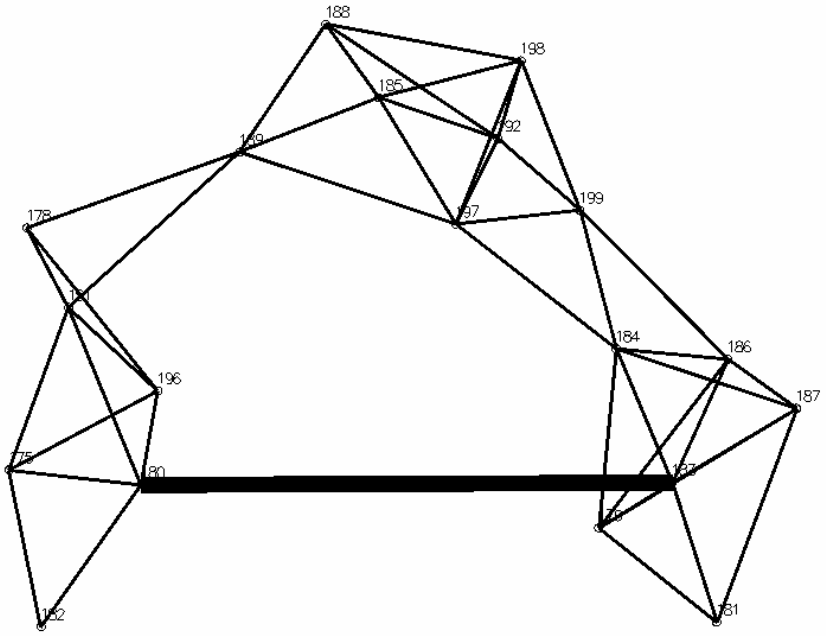

Figure 1 – Self-Contained In-Band Wormhole in a 19-Node OLSR MANET

3. METRICS FOR GRAVITATIONAL CHART ANALYSIS

In this section, we introduce several new metrics for in-band wormhole analysis that expand the basic gravitational analysis metrics. These metrics do not focus solely on individual node source/destination paths as those in [KSG06], but instead attempt to evaluate the overall effects of the in-band wormhole on a specific node or on the entire topology. We organize these new metrics into three metric families: *path-specific* (Section 3.1), *node-specific* (Section 3.2), and *topology-general* (Section 3.3). Node-specific metrics analyze the effects of a specific wormhole configuration on the individual nodes within the topology; topology-general metrics evaluate the wormhole's effects on the topology as a whole.

In some cases, metrics from one family can be applied or extended to another with some modifications. For example, the node-specific metric, *node-cost* (Section 3.2), can be derived from the *cost* path-specific metric. Also, metrics within a family can be derived from one another to form new metrics with additional meaning. Computing a mean value of another metric is one such example.

In the following metric equations, some common terminology is used. T is the set containing all nodes, edges, and paths within a topology. The set of all reachable paths in a given topology T for node N_i is represented by the set S_{Ti}. Each reachable source-destination path in S_{Ti} from N_i to some other node N_j,, is donated by P_{ij}.

$$S_{T_i} \in T$$

$$P_{ij} \in S_{T_i}$$

Throughout our metric descriptions, we use subscripts to indicate the family the metrics belong to, including: P_{ij} for path-specific, N_i for node-specific, and T_i for topology general.

3.1 Path-Specific Metrics

In addition to the path-specific metrics defined in [KSG06], we define a new metric that normalizes the cost of a wormhole on a given path.

Relative cost is the normalized cost on a selected source-destination pair. The cost or penalty imposed by a wormhole on a path (C) is normalized using the normal non-wormhole cost (A).

$$RC_{P\,ij} = \frac{C_{P_{ij}}}{A_{P_{ij}}}$$

3.2 Node-Specific Metrics

In this section, we present several metrics that measure the impact of an in-band wormhole on specific nodes within a MANET. They allows us to understand the risk posed to vital servers or other critical nodes by an in-band wormhole attack. It also allows us to compare the effects between nodes to better understand how the wormhole influences routes within the MANET. These

new metrics are an extension to the basic in-band wormhole metrics introduced in Section 2.

Number of paths affected identifies the number of paths for node N_i in S_{Ti} that are influenced by the wormhole's shortest path illusion.

$$PA_{N_i} = \text{total number of affected paths for } N_i$$

Node cost is the cost of additional hops (C-A) imposed by the wormhole on all source-destination paths, P_{ij}, in S_{Ti} for node N_i :

$$Cost_{N\,i} = \sum_{P_{ij} \in S_{T_i}} |\,(C_{P_{ij}} - A_{P_{ij}})\,|$$

Mean node cost is the average cost imposed by a wormhole on the affected paths of node N_i where n_i is the number of paths affected for N_i:

$$\overline{Cost_{N\,i}} = \frac{Cost_{N_i}}{n_i} = \frac{\sum_{P_{ij} \in S_{T_i}} |\,(C_{P_{ij}} - A_{P_{ij}})\,|}{n_i}$$

Node relative cost is the normalized cost on a given node. The cost or penalty imposed by a wormhole on a path (C) is normalized using the normal non-wormhole cost (A).

$$RC_{N\,i} = \frac{\sum_{P_{ij} \in S_{T_i}} C_{P_{ij}}}{\sum_{P_{ij} \in S_{T_i}} A_{P_{ij}}}$$

Node attraction (AT) is the sum of the attraction (A-B) felt by a node as the result of a wormhole on all of its source-destination paths.

$$AT_{N\,i} = \sum_{P_{ij} \in S_{T_i}} |\,(A_{P_{ij}} - B_{P_{ij}})\,|$$

Attraction is a measure of the resiliency of the wormhole to changes in topology. If the strength of attraction is small, then a small improvement in the normal path length could cause routing algorithms like OLSR to chose the normal path instead of the wormhole path.

Mean node attraction is the average *node attraction* (AT) for node N_i across its affected paths, n_i.

$$\overline{AT_{N\,i}} = \frac{AT_{N_i}}{n_i} = \frac{\sum_{P_{ij} \in S_{T_i}} |\,(A_{P_{ij}} - B_{P_{ij}})\,|}{n_i}$$

Node relative attraction (RAT) is a normalized measure of the penalty incurred by a specific node, N_i, from using the in-band wormhole link in a given topology. It is computed as the sum of the normal paths lengths for a node divided by the sum of the perceived path lengths. The normalization allows for a more straightforward comparison between topologies.

$$RAT_{N_i} = \frac{\sum_{P_{ij} \in S_{T_i}} (A_{P_{ij}})}{\sum_{P_{ij} \in S_{T_i}} (B_{P_{ij}})}$$

Node detectability (ND) is the sum of the individual path measurements for detectability (C-B) for all the reachable paths for node N_i.

$$ND_{N\,i} = \sum_{P_{ij} \in S_{T_i}} |\,(C_{P_{ij}} - B_{P_{ij}})\,|$$

Detectability is a measure of the disparity between the perceived path length through the wormhole (B) and the actual path length (C). A large disparity between these measurements is used as a detection mechanism in [KSG06].

3.3 Topology-General Metrics

In this section, we present several metrics that measure the impact of an in-band wormhole on specific MANET topologies. Using these metrics, we can compare and rank wormhole topologies against one another and look for topological characteristics responsible.

Overall number of nodes affected is the total number of nodes in a given topology that have at least one path affected by a specific in-band wormhole.

n_T = total number of affected nodes in topology T

Overall number of paths affected (PA) is the total number of source-destination paths affected by a specific in-band wormhole for a given topology.

$$PA_T = \sum_{N_i \in T} n_i$$

Overall relative cost (RC) is an overall measure of the penalty incurred by a topology, *T*, from using the fictitious paths presented by in-band wormhole. It is computed as the sum of the *node relative cost (RC)* values for all nodes in the topology.

$$RC_T = \sum_{N_i \in T} (RC_{Ni})$$

Overall mean node cost is the average cost imposed by a wormhole on the affected paths of node N_i where n_i is the number of paths affected for N_i:

$$\overline{Cost_T} = \sum_{N_i \in T} (\overline{Cost_{Ni}})$$

Overall relative degree of attraction (RAT) is an overall measure of the penalty incurred by a topology, *T*,

from using the fictitious paths presented by an in-band wormhole. It is computed as the sum of the *node relative attraction (RAT)* values for all nodes in the topology.

$$RAT_T = \sum_{N_i \in T} (RAT_{Ni})$$

4. TESTING

To assess the potential utility of our expanded metrics for the gravitational analysis methodology, we made use of a 19-node emulated MANET running the OLSR protocol. Section 4.1 describes the test environment and procedure. Section 4.2 uses the expanded metrics to examine node placement in two topologies, where only the wormhole location is changed; and Section 4.3 discusses specific topological configurations and relates them to the expanded metrics. While Section 3 defined several new metrics for wormhole analysis, we only discuss a subset of the node and topology metrics in this paper.

4.1 Test Environment and Procedure

Our laboratory test environment employs 19-nodes, all of which run the Fedora Core 3 operating system and the OLSR protocol. The scenario consisted of 61 random movement topologies which were enforced via packet filter rules. The movement of the nodes was somewhat restricted to increase the likelihood that the generated topologies will be conducive to wormholes. We encourage node movement within horseshoe-like topologies by creating "no-fly zone" into which nodes could not wander. Also, we fixed the positions of the 3 attacking nodes, spacing them approximately like the vertices of an equilateral triangle.

To perform accurate, real-time gravitational analysis, our experiments made use of an Army Research Laboratory (ARL) developed *gravitational analysis* tool to trace and record the reachable routes for all nodes in the topology using the "Record Route" feature of ping, i.e. *ping –R*. The tool allows us to accurately determine which paths traveled through the wormhole and which paths ignored it. For each topology, we performed gravitational analysis by:

1. Allowing the topology time to stabilize without a wormhole;
2. Recording all paths in the topology using the gravitational analysis tool;
3. Setting up a self-contained in-band wormhole using three attackers (nodes 180, 183, and 185) and then allowing the topology time to settle; and
4. Recording all paths in the topology using the gravitational analysis tool.

The gravitational analysis tool then uses the recorded pre/post wormhole path information to generate a topology-specific gravitational chart. This procedure was repeated for each of the 60 topologies in the scenario. We then computed the path-specific, node-specific, and topology-general metrics described in Section 3 from each gravitational chart. The results were then used to analyze wormhole impact on nodes, individual topologies, and the scenario as a whole.

4.2 Analysis of Node Placement Within a Topology

Table 2 shows several of the node specific metrics computed, as described in Section 3, from the gravitational chart shown in Table 1.

Table 2: Metrics Computed From Table 1

Node:	#Paths Aff:	Cost:	$\overline{\text{Cost}}$:	RC:	AT:	RAT:
175:	07	22	3.143	1.373	13	1.283
178:	05	23	4.600	1.469	02	1.043
179:	06	19	3.167	1.352	11	1.256
181:	06	13	2.167	1.188	17	1.327
182:	09	25	2.778	1.333	20	1.364
184:	05	19	3.800	1.452	06	1.167
186:	05	14	2.800	1.275	11	1.275
187:	06	19	3.167	1.352	11	1.256
188:	00	00	0.000	1.000	00	1.000
189:	01	05	5.000	1.132	00	1.000
191:	05	18	3.600	1.391	07	1.179
192:	00	00	0.000	1.000	00	1.000
196:	06	17	2.833	1.288	13	1.283
197:	00	00	0.000	1.000	00	1.000
198:	00	00	0.000	1.000	00	1.000
199:	02	08	4.000	1.186	02	1.049

As shown in Table 2, node 182 exhibits both the largest *number of affected paths* (i.e. 9) as well as the greatest *node cost* (i.e. 25) for this particular topology. As depicted in Figure 1, node 182 is positioned at the base of the topology and is a direct 1-hop neighbor of a wormhole-end attacker. It is also located on the left side of this topology which has a lower node density than the right side. A node in this situation is especially vulnerable to the effects of the wormhole due to its distance from all other nodes and proximity to a wormhole-end. Node 182, therefore, exhibits the largest node attraction (AT) and relative node degree of attraction (RAT) values of any other node in the topology (i.e., 20, 1.364). Consequently, node 182 chooses the wormhole path for 9 of the 15 possible destinations in the topology (excluding the attacker nodes).

Although node 182 exhibits a larger cumulative cost for this topology, node 178 is shown to have a higher mean node cost ($\overline{Cost_{N_i}}$), per path, over its five affected paths (i.e., 4.600 vs. 2.778). The fact that node 178 is closer to the intermediate colluder than the near wormhole-end accounts for this seemingly contradictory result. Wormhole traffic from node 178 must first travel to the near wormhole-end attacker where it is encapsulated and tunneled to the intermediate colluding attacker, node 185. When the victim node occupies a position in the topology along a path to the intermediate colluder and is closer to the intermediate colluder than the

near wormhole-end attacker (as is node 178 compared to attacker node 180), the wormhole traffic will travel in a semi-loop, from the victim node to the near wormhole-end attacker to the middle colluder, imposing additional hops to the already lengthy wormhole path. This semi-loop penalty occurs on both ends of the wormhole if both source and destination lie along a path to the middle colluder and are closer to the middle colluder than their corresponding wormhole-end attacker.

Conversely, nodes 188, 192, 197, and 198 are shown to be unaffected by the wormhole in Table 2. These nodes are in the unique topological position such that, in the absence of a wormhole, they are 1-hop closer to one wormhole-end attacker than to the other. With the wormhole in place, they could possibly select either the pre-wormhole path or the wormhole path, with equal cost, to reach the far wormhole-end attacker node. In this case the routing protocol will choose the wormhole path with 50% probability. Tables 1 and 2 above show that the routing protocol on nodes 188, 192, 197, and 198 chose to use the pre-wormhole path, leaving these nodes unaffected by the wormhole. Node 189, also in the same topological position as the aforementioned nodes (Figure 1), is shown to be affected by the wormhole (for the same reasons discussed above), however, in this case the routing protocol has chosen to use the wormhole for one path as indicated by Table 2.

As a second example, Tables 3a and 3b present the metrics computed for both wormhole configurations depicted in Figure 2 below.

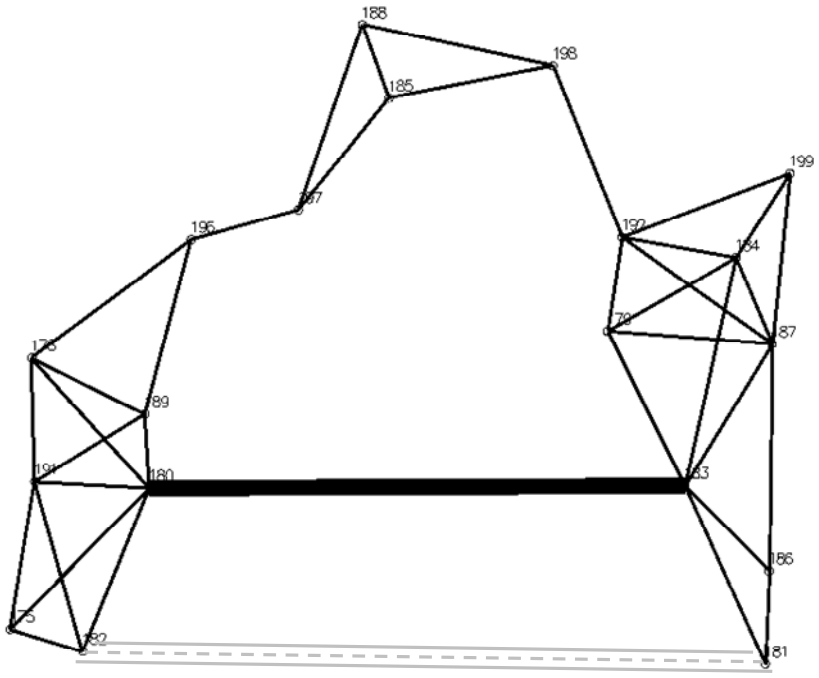

Figure 2 –Self-Contained In-Band Wormhole in a 19-Node OLSR MANET

a) Wormhole between attacker nodes 180 and 183 (solid line)

b) Wormhole between attacker nodes 182 and 181 (dashed line)

Table 3a – Wormhole Metrics, Figure 2, Topology 2a

Node:	#Paths Aff.:	Cost:	$\overline{\text{Cost:}}$	RC:	AT:	RAT:
175:	09	20	2.222	1.206	43	1.796
178:	08	30	3.750	1.423	26	1.578
179:	07	23	3.286	1.333	26	1.605
181:	08	15	1.875	1.158	41	1.759
182:	09	20	2.222	1.206	43	1.796
184:	07	23	3.286	1.338	26	1.619
186:	07	16	2.286	1.198	33	1.688
187:	07	23	3.286	1.343	26	1.634
188:	00	00	0.000	1.000	00	1.000
189:	08	30	3.750	1.423	26	1.578
191:	09	29	3.222	1.354	34	1.708
192:	06	29	4.833	1.492	13	1.283
196:	07	38	5.429	1.603	11	1.212
197:	02	12	6.000	1.207	02	1.036
198:	03	18	6.000	1.321	03	1.057
199:	07	30	4.286	1.423	19	1.365
Topo:	104	356	3.423	1.307	372	1.471

Table 3b – Wormhole Metrics, Figure 2, Topology 2b

Node:	#Paths Aff.:	Cost:	$\overline{\text{Cost:}}$	RC:	AT:	RAT:
175:	08	35	4.375	1.361	37	1.617
178:	06	40	6.667	1.563	14	1.246
179:	06	37	6.167	1.536	17	1.327
180:	08	43	5.375	1.524	29	1.547
183:	07	33	4.714	1.418	30	1.612
184:	06	37	6.167	1.544	17	1.333
186:	07	33	4.714	1.407	30	1.588
187:	06	37	6.167	1.552	17	1.340
188:	00	00	0.000	1.000	00	1.000
189:	06	40	6.667	1.563	14	1.246
191:	08	43	5.375	1.524	29	1.547
192:	04	29	7.250	1.492	07	1.135
196:	03	22	7.333	1.349	05	1.086
197:	01	08	8.000	1.138	01	1.018
198:	01	08	8.000	1.143	01	1.018
199:	04	25	6.250	1.352	11	1.183
Topo:	81	470	5.802	1.416	259	1.297

Figure 2 depicts two distinct topologies; topology 2*a* in which the wormhole link appears between attacker nodes 180 and 183, and topology 2*b* in which the wormhole link appears between attacker nodes 182 and 181. As indicated in Tables 3a and 3b, the number of paths affected by the wormhole decreases overall from topology 2*a* to topology 2*b (81 vs. 104)*. This is a direct result of the wormhole moving 1-hop further from most nodes in topology 2*b* as compared to its initial position in topology 2*a*, and makes the wormhole less attractive as a shortcut. The general decrease in node attraction (AT) and relative node degree attraction (RAT) values from topology 2*a* to topology 2*b* affirms this result.

Although less attractive as a shortcut, the cost, mean node cost ($\overline{Cost_{N_i}}$), and relative cost (RC) to individual nodes increases overall from topology 2*a* to topology 2*b*, and is due to the same semi-loop path penalty discussed in the previous example. Because the wormhole-end attackers occupy the furthest points from the middle colluder, more nodes in topology 2*b* incur the semi-loop penalty than in topology 2*a*. Traffic from all nodes affected by the wormhole will travel in the "wrong direction", both initially to reach a wormhole-end and upon wormhole exit to reach the destination node.

In both topologies depicted in Figure 2, only node 188 escapes the influence of the wormhole. This node essentially mirrors the location of the middle colluder and is symmetric with respect to the two wormhole-end attacker nodes. The wormhole path is not attractive to a node in this location since its use results in longer paths for all destinations compared to the non-wormhole paths.

4.3 Topology Analysis

In total, the wormhole scenario evaluated in this paper consisted of sixty-one separate topologies, of which only thirty-eight were wormhole capable. The remaining twenty-three topologies were either disjoint, or formed links such that the middle colluder was asymmetric with respect to the wormhole-end attackers, resulting in wormhole instability and collapse. The random motion of the non-attacker nodes was constrained in generating the test topologies to facilitate wormhole formation, so these results may not generalize to topologies with unrestricted random motion. Further, of the thirty-eight wormhole-capable topologies, the number of paths affected ranged from 17% to 32% (in the worst case) of the possible 342 reachable paths per topology. The mean number of paths affected was 83 paths (24% of possible paths).

Figure 3 shows a sampling of six different topology configurations (A-F) of the thirty-eight wormhole capable topologies that represent characteristics of the larger group. The large black dots indicate the attacker positions, while the thick black lines identify the fictitious wormhole link.

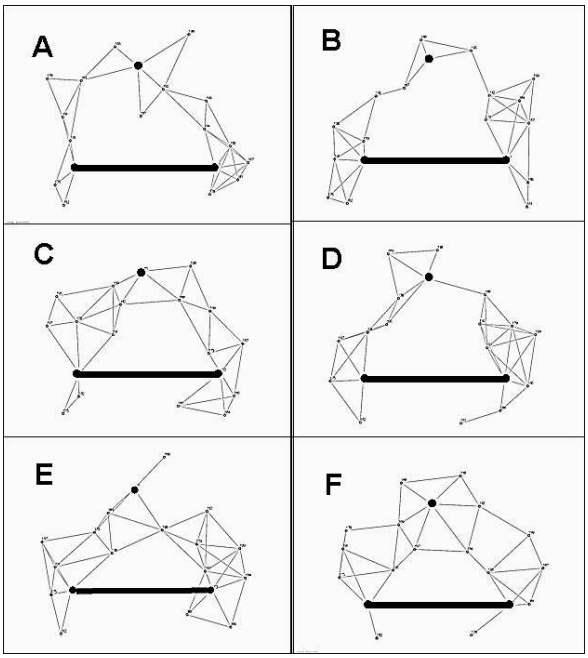

Figure 3 – Sample Topologies A - F

In topology 3B, most nodes cluster around the wormhole-end attackers, leaving a long, sparse path connecting network segments (a dumbbell shape). This type of topology is especially vulnerable to the effects of a wormhole since, to the majority of non-attacker nodes the wormhole will appear to be the shortest path between network segments. Consequently, topology 3B contains the largest number of affected paths in the scenario. Topology 3D also exhibits similar characteristics as topology 3B, however, shows an increased distribution of nodes along the path connecting the wormhole ends, lowering it's overall number of paths and nodes affected by the wormhole.

Topologies 3A, 3E, and 3F exhibit opposite characteristics as those of 3B and 3D. In these topologies nodes show a more diverse distribution and do not cluster largely around the wormhole-end attackers. Consequently, these topologies exhibit fewer paths and nodes affected by the wormhole. Also, in topologies 3E and 3F, the distance between network segments is small allowing many nodes to reach the far network segment in fewer or the same number of hops as using the wormhole path. Topology 3C exhibits the largest number of nodes affected than all other topologies shown in Figure 3. In fact, all non-attacker nodes are shown to be affected by the wormhole. Though topologies 3C and 3F may appear visually similar, in topology 3C most nodes are located nearer to the wormhole-end attackers as opposed to topology 3F where nodes are more centrally located, accounting for the larger number of nodes and paths affected in topology 3C. Table 4 presents several topology general metrics computed for the topologies depicted in Figure 3.

Table 4 – Wormhole Metrics, Figure 3 A-F

Topology	# Paths Aff.	# Nodes Aff.	Cost	$\overline{\text{Cost}}$
A	63	12	202	3.206
B	104	15	356	3.423
C	93	16	283	3.043
D	86	15	223	2.593
E	78	13	286	3.667
F	72	13	220	3.056

5. CONCLUSIONS

Gravitational analysis has been shown to be an effective tool for analyzing the impact of in-band wormholes on a MANET. In this paper, we have enhanced the gravitational analysis technique by adding new metrics measuring the overall impact of a wormhole on individual nodes as well as metrics measuring the impact on the overall topology under attack. These new metrics give us insight into attacker placement, topology vulnerability, and overall wormhole impact. Using these metrics in combination with gravitational charts, we can easily identify those topologies that are most/least impacted by the wormhole and assess the specific topological characteristics responsible. This is of particular importance in a MANET where resources to defend against such an attack may be limited. By understanding the real impact of the in-band wormhole attack, we can gain a better understanding of the threat posed by the attack and apply the appropriate countermeasures according to that threat.

6. FUTURE WORK

Our future work will include further experiments to examine and validate our metrics under a broader set of test conditions. We will continue to develop new metrics that associate priorities and/or weights with selected source-destination paths. This will allow us to more easily and selectively monitor the wormhole effects on traffic to and from critical nodes in the network. We also intend to examine scenarios where the wormhole attackers move within the topology while all other nodes are static. By moving only the attackers, we can examine the effects of different wormhole configurations on a specific topology. From this analysis, we hope to learn more about the resilience of the in-band wormhole attack and identify the optimal countermeasure for such an attack. In addition to increasing the realism of the single wormhole experiments, we plan to extend the experiments to include multiple wormholes and/or additional colluding nodes.

REFERENCES

[ADJ05] C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, D. Raffo, "Securing the OLSR routing protocol with or without compromised nodes in the network", Institut National de Recherche en Informatique et en Automatique", ISRN INRIAR/RR-54-94, February 2005.

[HU03] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", In Proceedings of IEEE Infocomm 2003.

[KSG06] P. Kruus, D. Sterne. R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic, and G. Lawler, "In-Band Wormholes and Countermeasures in OLSR Networks", Proceedings of the Second International Conference on Security and Privacy in Communication Networks, SecureComm 2006, Baltimore, MD, Aug. 28 - Sep. 1, 2006.

[OLSR03] "Optimized Link State Routing (OLSR)," IETF RFC 3626, T. Clausen, P. Jacquet, Ed., October 2003.