**A Wireless Protocol to Prevent Wormhole Attacks**

A Thesis
in TCC 402

Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment

of the Requirements for the Degree
Bachelor of Science in Computer Engineering

by

Jackson Kwok

March 23, 2004

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in TCC Courses.

_____

Approved _____ Date_____
Technical Advisor – David Evans

Approved _____ Date_____
TCC Advisor – Claire Chantell

## Preface

I would like to thank Professor David Evans, my Technical Advisor, for his support and advisory work during the course of this project, and Professor Claire Chantell for her aid as my TCC advisor. I would also like to thank Lingxuan Hu, a graduate student in the computer science department for contributing source code and documentation necessary to produce this project. Also, I like to credit the computer science department providing me with resources and network disk space, for which I am very grateful.

# Table of Contents

# List of Figures

## Glossary of Terms

*Asymmetric Key Cryptography* – also known as public key encryption. Relies on a pair of public and private keys to encrypt and decrypt messages sent across the network.

*Denial of Service (DoS) attack* – an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

*Global Positioning System (GPS)* – a system that reports its geographic location using satellites orbiting the earth. The location accuracy is anywhere from 100 to 10 meters for most equipment. Accuracy can be pinpointed to within one (1) meter with special military-approved equipment.

*hop count* – the number of nodes a *packet* travels from a sending node to a receiving node.

*network* – any series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub networks.

*nodes* – a connection point on a network. Possible nodes may include network devices such as a computer, laptop, hub or router.

*packet* – a unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

*protocol* – a special set of rules to be followed on a computer network. For example, Hypertext Transfer Protocol (HTTP) governs how to transfer data on the World Wide Web.

*selective forwarding* – a technique that allows nodes to refuse forwarding certain packets and simply drop them, ensuring that they are not propagated any further in the network.

*Symmetric Key Cryptography* – also known as shared key encryption. Relies on the secrecy of one key between two nodes to encrypt and decrypt messages in the network.

*wormhole* – a tunnel in a network which allows signals from nodes to travel faster than normal. This is similar to the definition of a wormhole in space which allows faster space travel.

*wormhole attack* – an attack done using one or more wormholes in a network. A successful attack may result in a disruption or breakdown of a network.

Source: http://whatis.techtarget.com

# Abstract

As an increasing number of people are going wireless, reducing the vulnerability of wireless networks is becoming a top priority. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful and preventing the attack has proven to be very difficult. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network.

This project designed and developed a new protocol that prevents wormhole attacks on wireless networks. The design of this protocol is based on the use of asymmetric and symmetric key cryptography and a Global Positioning System (GPS). It was evaluated using simulations under realistic ad-hoc network settings. The simulations identified the strengths and weaknesses of this protocol under different distributions of GPS and non-GPS nodes, network areas and network structures. Within a set of requirements and assumptions, this wireless security protocol can detect nearly half of wormhole attacks by relying on each node's relative location.

# Chapter 1: Introduction

## A. Thesis Statement

The increasing popularity and usage of wireless technology is creating a need for more secure wireless networks. Wireless networks are particularly vulnerable to a powerful attack known as the wormhole attack. This project researched and developed a new protocol that prevents wormhole attacks on a wireless network. A few existing protocols detect wormhole attacks but they require highly specialized equipment not found on most wireless devices. This project aims to develop a defense against wormhole attacks that does not require as a significant amount of specialized equipment. In this new protocol, only a subnet of nodes requires a Global Positioning System (GPS), which enables the network devices to detect their own location. The thesis of this project suggests that the collaboration between GPS and non-GPS nodes can provide adequate detection of wormhole attacks in a wireless network. The analysis of this project's results may present valuable insight for new approaches in handling wormhole attacks in the field of wireless security.

## B. Problem Definition

Ad-hoc or spontaneous wireless networks are threatened by a powerful attack known as the wormhole attack. A wormhole attack can be set up with relative ease, but preventing one is difficult. To set up a wormhole attack, an attacker places two or more transceivers at different locations on a wireless network as shown in Figure 1.

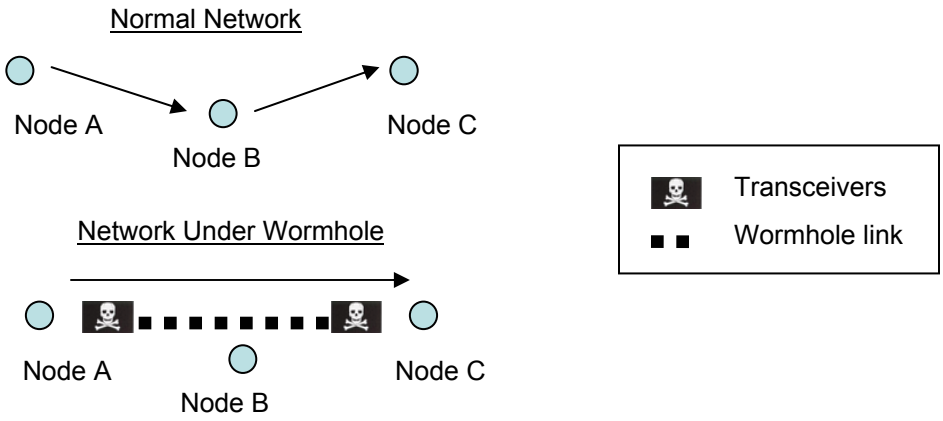


**Figure 1: Set-up of a wormhole**. Node A can reach node C within a shorter time with the help of a wormhole.

This establishes a wormhole or tunnel through which data can transfer faster than it could on the original network. After setting up a wormhole, an attacker can disrupt routing to direct packets through the wormhole using a technique known as selective forwarding depicted in Figure 2. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network as shown in Figure 3 [4: 3].

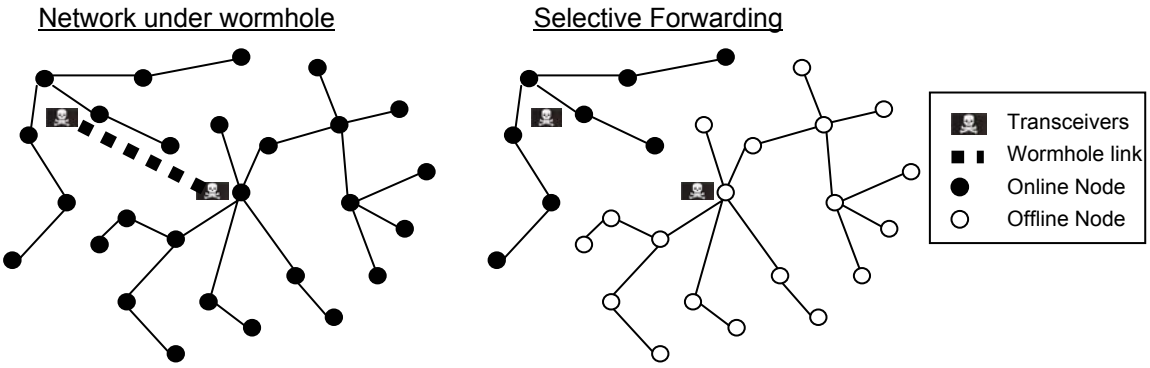


**Figure 2: Selective Forwarding**. Lower right portion of network relies on wormhole link to route information. Disconnecting wormhole link results in breakdown of the network.

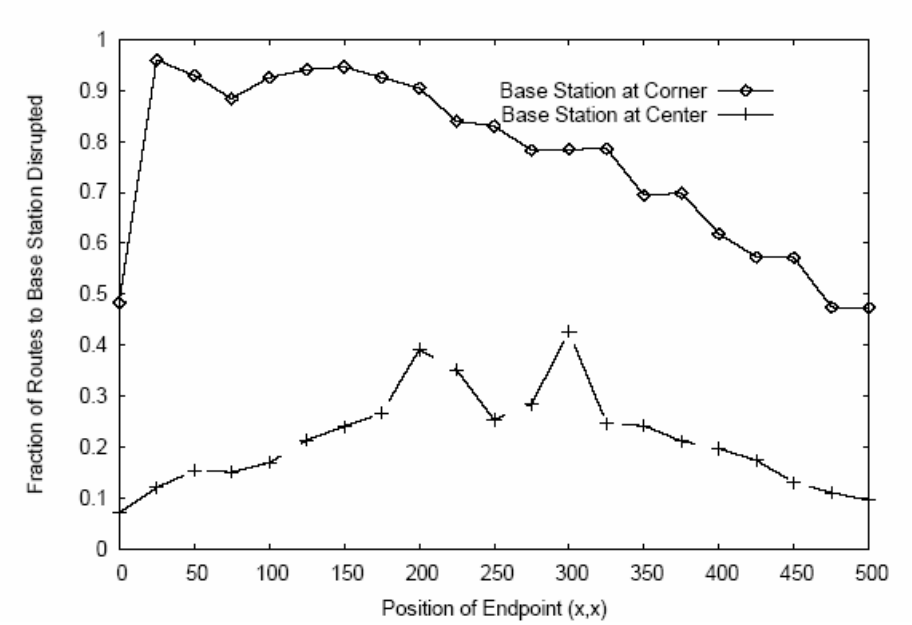


**Figure 3: Strategic Placement of Wormhole.** The routes to the base station are disrupted the closer the wormhole endpoints are to the base station [4: 3].

Wireless networking is a young technology and thus, many wireless network devices have not been designed to defend against wormhole attacks. For example, a sensor network device called the Mica mote has the ability to sense information about its surroundings such as temperature, sound or movement [9: 1]. Supplied with a 4 MHz processor, 512KB flash memory and two AA batteries, the Mica mote has little room for security measures to protect itself from a wormhole attack [9: 1].

Current network protocols are also vulnerable to wormhole attacks. Protocols are a special set of rules that nodes follow on a network. Nodes or network devices such as laptops, computers or the Mica mote explained above, currently do not follow rules that help them detect wormhole attacks. Cryptography, which is used widely to secure transfer of information in protocols, will not prevent wormhole attacks. As a result, this project advocates the need for new set of protocols for wireless networks.

## C. Background and Previous Work

Several techniques such as localization schemes and packet leashes can possibly prevent wormhole attacks. Localization systems verify the relative locations of nodes in a wireless network [4: 2]. Packet leashes restrict the packet's maximum allowed distance of transmission [6: 4]. Published research describes protocols that use directional antennas, ultrasonic signals and other additional equipment to prevent wormhole attacks. These techniques and specialized equipment may help detect wormholes in wireless networks and therefore prevent wormhole attacks. A detailed review of these techniques appears in chapter two.

## D. Rationale and Scope of the Project

Wireless networks are currently very insecure and thus, they are easy targets for attackers. Major users of wireless systems, such as the military, government, emergency response teams and businesses can fall prey to these threats. Ideally, all wireless networks would be protected from wormhole attacks. Existing wireless security protocols have been able to block some but not all wormhole attacks. In these protocols, there are compromises between performance and security. This project provides an overview of the available protocols and offers an alternative solution which can reduce the risk of a wormhole attack. This alternative protocol can be implemented and simulated under reasonable requirements of cost and usability. This report also includes a discussion and recommendation for further research on this topic. Users of wireless network technology and applications such as sensor networks should benefit significantly from continued research in this field.

## E. Overview of the Report

Chapter two provides a review of previous work in preventing wormhole attacks. Chapter three discusses the protocol design. Chapter four describes experiments conducted by this project and using the results, evaluates the extent of the protocol's ability to prevent wormhole attacks. Chapter five draws a conclusion and recommends ideas for future work to prevent wormhole attacks.

# Chapter 2: Background and Previous Work

This chapter discusses previous work on preventing wormhole attacks. All protocols in this section fall under two broad categories: localization schemes and packet leashes.

## A. Localization Schemes

Wireless security protocols based on localization have the potential to detect wormhole attacks [4: 2]. Localization systems are based on verifying the relative locations of nodes in a wireless network [4: 2]. Knowing the relative location may help conclude whether or not packets are sent by either a node or wormhole. Several localization schemes discussed in this section: Echo Protocol, Area-based Point Triangulation Test (APIT), Coordinate System, Signal Strength and Infra-Red (IR), and Directional Antennas.

Sastry, Shankar and Wagner from the University of California at Berkeley discuss a location verification scheme known as the Echo protocol [16: 1]. Rather than focusing on individual nodes of a network, this protocol emphasizes the regions of verification [16: 3]. Nodes in the regions of verification must prove they are part of the wireless network using radio frequency (RF) and ultrasonic sound capabilities [16: 3]. A verified node sends a RF signal to an unverified node in the network. To prove it is part of the network, the unverified node sends an ultrasonic signal back to the verified node. The verified node determines whether or not the unverified node is in the region of verification depending on the time it takes to receive an ultrasonic signal [16: 5]. RF signals are used in most wireless network devices today. The strong points of this

protocol are that cryptography and tight time-synchronization are not needed. However, because each network device needs additional equipment to detect and emit ultrasonic sound frequencies, this protocol may detract some developers from adopting this idea to prevent wormhole attacks.

He, Huang, Blum, Stankovic and Abdelzaher developed an area-based point in triangulation test (APIT) which uses triangulation to determine the location of nodes in a network [2: 1]. Calculations are performed to check whether or not certain nodes are within triangles formed by anchors, which are nodes with Global Positioning System (GPS) [2: 3]. These calculations determine the relative locations of all nodes in the network which may prove helpful to combating wormhole attacks. Compared to the Echo protocol, APIT does not require additional equipment for ultrasonic sound frequencies. However, APIT does require some nodes to have GPS in the wireless network to give some reference of locations in a network so that nodes without GPS have a relative idea of where they stand [2: 1].

Another localization scheme known as the coordinate system involves the work done by Nagpal, Shrobe and Bachrach at Massachusetts Institute of Technology (MIT) [10: 1]. Similar to the APIT, the protocol uses a subset of GPS nodes to provide nodes without GPS a sense of relative location [10: 2]. This is achieved using two algorithms: the gradient which measures a GPS node's *hop count* from a point in a network, and multilateration, which determines the way GPS nodes spread information of its location to nodes without GPS [10 3-4]. Hop counts tell how far a node is from a particular source. A flaw in using this scheme is that wormholes can disrupt hop counts within a

network [5: 2]. Therefore, any system following this scheme is rendered defenseless under wormhole attacks.

Bulusu, Heidemann and Estrin discuss other localization techniques such as the verification of signal strength and Infra Red (IR) [1: 3]. Weaker signal strengths may indicate a node is farther away. However, signal strengths are not reliable outdoors because ambient sound can disrupt signals [1: 3]. IR is very efficient in pinpointing nodes in open spaces using invisible lasers. On the other hand, IR is very sensitive to its surroundings rendering it unusable outdoors due to the interference of sunlight and indoor areas which do not have a line-of-sight to each network device [1: 3].

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks [5: 1]. Directional antennas are able to detect the angle of arrival of a signal [5: 1]. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east) [5: 4]. This protocol falls only if the attacker strategically placed wormholes residing between two directional antennas [5: 7]. This problem has been solved by having a verifier check on the communications between two nodes [5: 8]. However, some legitimate nodes are invalidated due to this solution. Drawbacks to this protocol include the flaw of rejecting valid nodes and requiring the use of directional antennas to prevent wormhole attacks.

Overall, localization schemes are very effective in determining location. Wormholes, which fake their location to appear to be in two or more places at once, may trigger protocols to reject them as invalid nodes.

## B. Packet Leashes

Hu, Perrig and Johnson developed protocols with packet leashes have been proven to be reliable wormhole attack detectors [6: 4]. Packet leashes place restrictions on a packet's maximum allowed transmission distance in a network [6: 4]. Two types of packet leashes discussed in this article are temporal and geographical leashes. Temporal leashes require tightly synchronized clocks on all nodes [6: 4]. Protocols based on temporal leashes ensure that packets transmitted across the network have an upper bound on its lifetime, which restricts the maximum distance of travel [6: 4]. Packets on a network remain valid for a certain time interval before they are rejected. However, setting up wormhole attacks under temporal leashes is difficult because packets must be sent through the wormhole within the restricted time period.

A geographical leash is the second type of leash discussed. Protocols based on geographical leashes differ slightly from temporal leashes in that each node must know its location and have loosely synchronized clocks [6: 4]. Using location and time, nodes can determine whether the packet is coming from a valid node or a wormhole. This protocol allows more flexibility in the synchronization time among nodes than temporal leashes [6: 5]. This type of packet leash also incorporates some of the same ideas used in localization schemes of using location to prevent wormhole attacks.

A more refined temporal leash protocol known as the TESLA with Instant Key disclosure (TIK) is discussed by Hu, Perrig and Johnson. TIK uses a hash tree to hold symmetric keys to authenticate nodes [6: 6-7]. Receiving nodes will be able to determine a packet's validity based on the time interval and the corresponding key of the sender node [6: 9]. TIK packets are structured so that the receiver node verifies the time interval

and message authentication codes (HMAC) before the key arrives. If the time interval is valid, then the node verifies the key [6: 9]. Completing both tests would verify the sender was not a wormhole. The TIK temporal leash protocol effectively detects a majority of wormholes. An attacker must know the right time intervals and keys pairs so that nodes in the wireless network will accept the wormhole's packet. A disadvantage of this protocol is its strict requirements in timing. Each node must be synchronized at exactly the same time and errors in time difference must not be larger than a few microseconds or even hundreds of nanoseconds [6: 4].

## C. Conclusion

Protocols based on localization schemes and packet leashes can prevent wormhole attacks. However, each protocol has different costs in achieving this goal. As mentioned before, temporal leashes require strict time synchronization among all nodes. As a result, this project focuses more on localization schemes and geographical leashes because it does not require tight time synchronization. However, the trade-off is that localization schemes and geographical leashes tend to use additional equipment. This project's design decisions will be discussed more in chapter three.

# Chapter 3: Protocol Design

The first section in this chapter will talk about the goals of this protocol. The second section will discuss the design of the network and network devices needed by the protocol. The third and final section will provide details on the protocol and how it works to detect wormholes.

## A. Goals

This protocol adopted several design decisions to meet certain goals. These goals were to design a protocol that not only prevents wormhole attacks but also:

1. Avoids using strict clock synchronization.
2. Limits the need for specialized equipment.
3. Ensures information confidentiality.
4. Provides high performance, low power consumption and minimal memory storage.

Using strict clock synchronization to detect wormhole attacks is impractical. It requires all nodes to synchronize within a few microseconds or hundreds of nanoseconds [6: 4], which involves the use of highly sensitive and expensive network devices. As mentioned in chapter two, localization schemes and geographic leashes can be used to avoid strict clock synchronization. Therefore, design decisions of this protocol are based on detecting wormholes using relative location rather than timing constraints.

Limiting the use of specialized equipment reduces the cost of creating a secure wireless network. Rather than requiring all nodes to have specialized equipment, this protocol uses a combination of GPS and non-GPS nodes to prevent wormhole attacks. Non-GPS nodes are equivalent to many nodes available off the shelf. An example of such a node would be the Mica mote discussed in chapter 1. GPS nodes on the other

hand would have all the properties of a non-GPS node except for the GPS. GPS were determined to be a low cost yet highly beneficial system compared to the use of other specialized equipment such as RF, IR and ultrasonic waves discussed in chapter 2.

While providing protection against wormhole attacks is the primary goal, this protocol has secondary goals to provide information confidentiality and integrity in addition to performance, power conservation and minimal data storage. The following paragraphs will discuss the designs of GPS, non-GPS nodes and the network environment for this protocol to achieve these goals.

## B. Design of the Network and Network Devices

### 1. Network Devices

The most significant difference between GPS and non-GPS nodes is that non-GPS nodes do not know their location directly. They rely on neighboring GPS nodes to determine their relative location. Otherwise, GPS and non-GPS nodes share many similar attributes. They use asymmetric and symmetric key cryptography and store a neighbor list and their transmission range distance in their memory.

Both types of nodes make use of asymmetric and symmetric key cryptography. Asymmetric key cryptography allows nodes to authenticate or verify the sender of the message. Since non-GPS nodes refer to GPS nodes to determine relative location, asymmetric key cryptography plays a crucial role to providing integrity and trust that only reports of location come from GPS nodes. Since all GPS nodes are the same, only one public key need to be preloaded into each node's memory to verify the identity of a GPS node.

Another disadvantage of asymmetric key cryptography is it requires nodes to send large packets of information, which reduces the bandwidth of the network. Encrypting and decrypting public and private keys also increases the power consumption of each node. To provide a faster form of communication, symmetric key cryptography is used rather than asymmetric key cryptography. Symmetric key cryptography uses smaller keys but also delivers the confidentiality needed to secure messages sent across the network. In symmetric key cryptography, each node holds keys for every other node in the network. Along with the GPS's public and private key, each node holds n – 1 symmetric keys, where n is the number of nodes in the network. Note that symmetric key cryptography requires nodes to be either preloaded with the keys in memory or to be distributed using a secure routing protocol. This project assumes that there is a separate routing protocol that handles this task. The emphasis of this project is to create a security protocol rather than an efficient routing protocol.

In addition to holding keys for cryptography, each node maintains a neighbor list. This neighbor list consists of all GPS or non-GPS nodes within the transmission radius of the node as shown in Figure 4. The node's transmission radius is also stored in memory for purposes explained in section C. Ideally, each node has a constant maximum transmission radius; however, in reality, network devices signals may vary depending on power consumption and other factors.

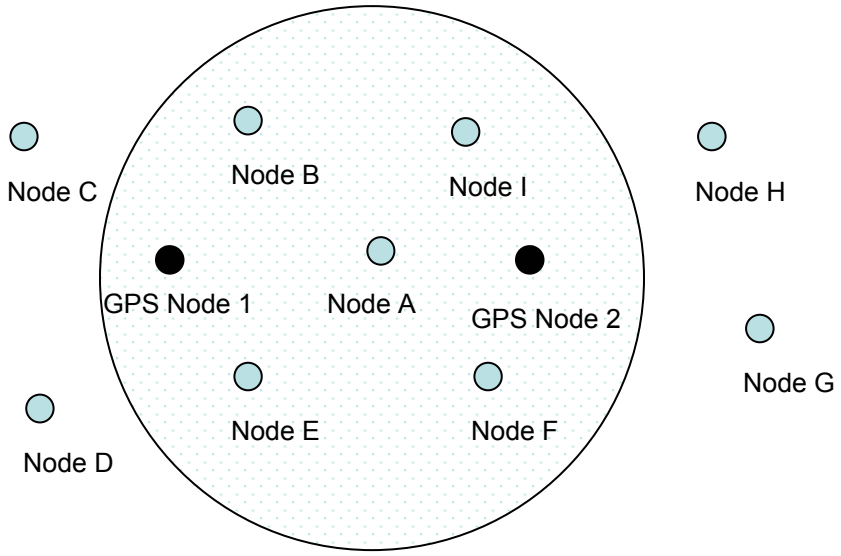


**Figure 4: Neighbor List**. Node's A transmission range includes nodes B, I, E and F and GPS nodes 1 and 2. The other nodes C, D, H, and G are not on node A's neighbor list.

**2. Network Environment**

The network environment requires that each non-GPS node must be in the transmission radius of at least one GPS node to prevent wormhole attacks effectively. However, the placement of nodes within the network does not matter. The network should work under ad-hoc or spontaneous networks. It should also work whether nodes in the network are mobile or stationary. An analysis of the optimal network environment will be discussed in-depth in chapter 5.

## C. Protocol Functionality

The design of this protocol relies on the collaboration of GPS and non-GPS nodes in the network. The following subsections will explain the initialization, communication and detection process of the protocol to identify wormhole attacks. A more formal description of this protocol is shown at the end of this chapter.

**1. Initialization Process**

Before the initialization process, all nodes are either sleeping or powered off. When the nodes are powered, the first step of the protocol is for the GPS node to broadcast or announce its presence in the network. GPS nodes will send this signal encrypted with a private key within its fixed transmission radius. All nodes within that radius will wake up, decipher the message using the GPS's public key, and respond to the broadcast using an encrypted message with their own identity. After all the nodes have responded, each node will have compiled a neighbor list of GPS or non-GPS nodes around their transmission radius. This list is stored in each node's memory.

Messages sent across the network include a nonce or random number generated depending on time of the message. These nonces are verified by the receiving node to ensure that they are not replays of previous messages. Without nonces, a wormhole attack can flood the network with messages to overwhelm the network as illustrated in Figure 5. This type of attack is also known as a Denial of Service (DoS) attack which is commonly used to bring down the services of websites by overloading it with service requests. Nonces prevent attackers from replaying previous messages and nodes from accepting these messages because only nonces with the appropriate time stamps are accepted.

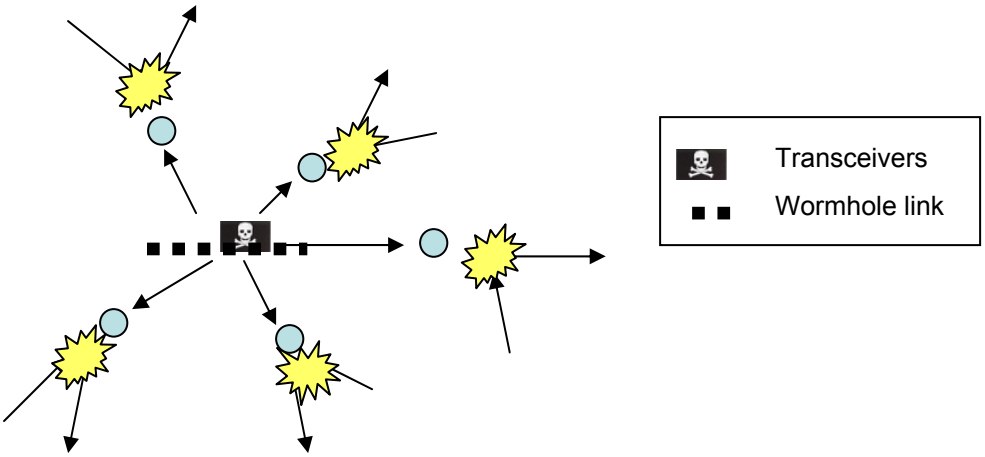


**Figure 5: Denial of Service (DoS) Attack.** A wormhole overwhelms nodes in the network with messages so that it cannot take other requests.

**2. Communication Process**

After the initialization process, all nodes should be able to forward messages to each other. To keep the communication confidential, each node encrypts its own message before sending it out to the network. As mentioned in section B, each node uses symmetric keys. Nodes in the network should remain in the communication state unless the one of the following conditions becomes true:

- One or more nodes move to a different location of the network.
- One or more nodes suddenly turn off or stop responding, requiring their removal from the network.
- One or more nodes suddenly turn on or arrive, requiring their addition to the network.
- The network has set a refresh rate that automatically brings the protocol back to initialization to update the network.

If one or more of these states becomes true, the protocol goes back to the initialization state to update each node's neighbor lists. Mobile networks may need to update at faster rates due to the constantly changing network structure. Higher refresh rates may help detect and prevent wormhole attacks but there are trade-offs in network performance and power consumption.

### 3a. Detection Process: One-Hop Calculation

Two calculations run in the background of the communication process to detect wormhole attacks. The first calculation determines whether or not a node in the network should be able to hear the GPS nodes in its list stored in memory. If the distance between any two GPS nodes in a node's neighbor list is greater than two times the transmission radius of the node, then the node is affected by a wormhole attack. A node can only hear GPS nodes at either end of the transmission radius as shown in Figure 6. Therefore, any GPS nodes whose distances are greater must be compromised by a wormhole. This calculation will be referred as the one-hop calculation throughout the rest of this report.

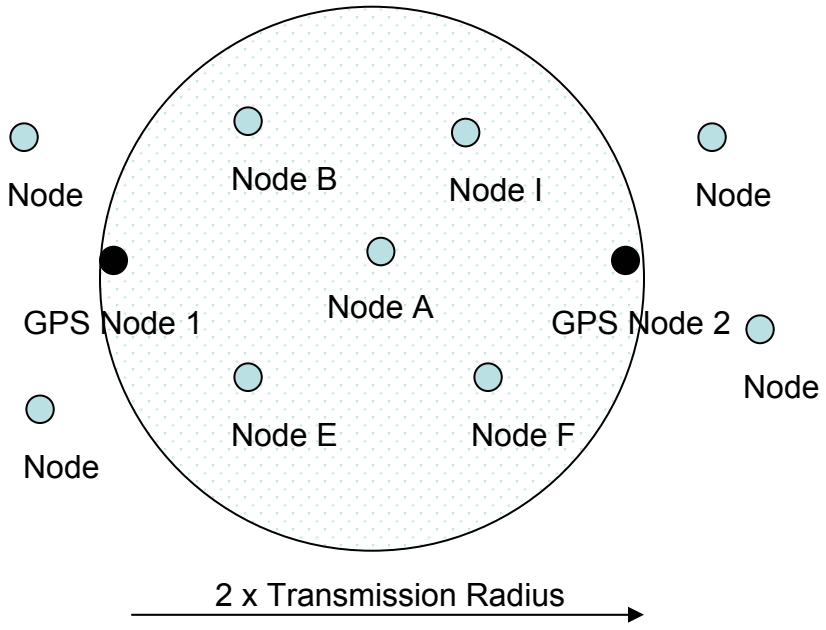


**Figure 6: One-Hop Calculation.** GPS nodes can only be 2 times the transmission radius away from each other in node A's neighbor list.

A hop count is the number of nodes which a sending node must forward packets to reach the receiving node. One-hop means that a sending node's packet can reach its destination within its transmission range as depicted in Figure 7.

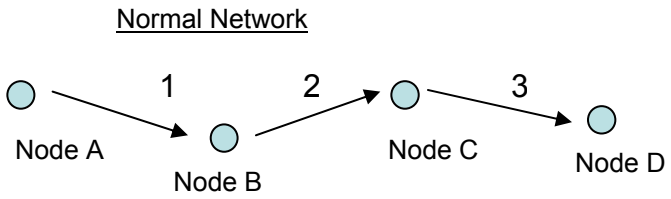


**Figure 7: Hop-Counts.** It takes one hop for node A to reach node B, two for node A to reach C, and three in order to reach node D.

### 3b. Detection Process: Two-Hop Calculation

The second calculation determines whether two nodes can communicate with each other. For example, suppose there are two nodes A and J that are within the transmission radius of each other. If the distance between any GPS node in node A's neighbor list and any GPS node in node J's neighbor list is greater than three times the transmission radius of the node, then both nodes are most likely subjected to a wormhole attack. A node can only communicate with another node with the maximum distance of the GPS nodes at the end of their transmission radiuses as illustrated in Figure 8. This

calculation will be referred as the two-hop calculation.

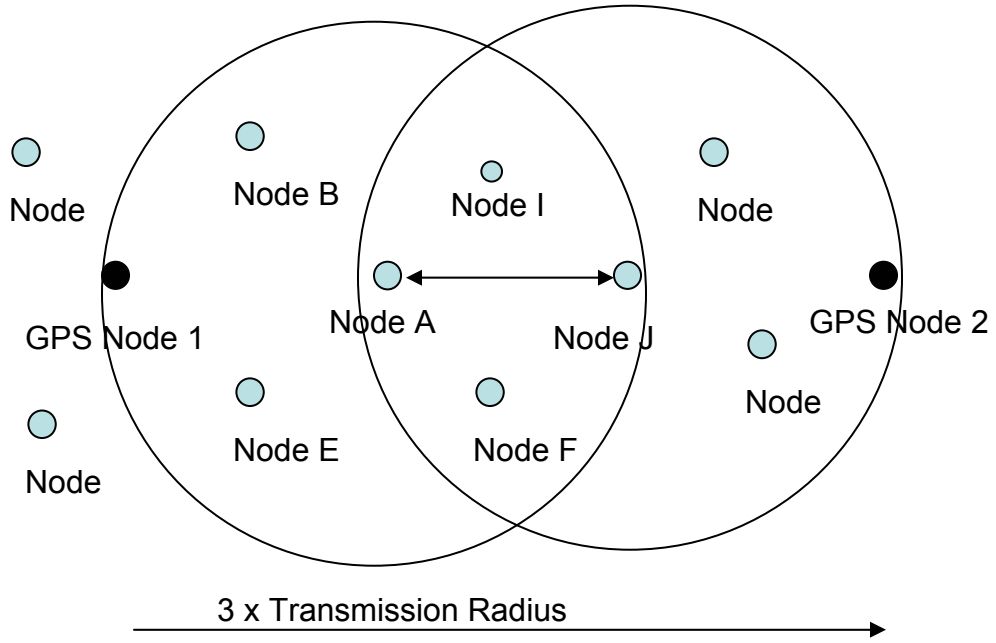


**Figure 8: Two-Hop Calculation.** When node A communicates with node J, node A checks its neighbor list with node J's neighbor list to see if there is any GPS nodes are greater than three times the transmission radius.

To summarize, nodes that fail the one-hop calculation are likely to be nearby a wormhole. Nodes that fail the two-hop calculation are potentially sending packets to a node compromised by a wormhole. In the detection process, any node failing the one-hop and two-hop calculations shut down and are removed to avoid additional damage on the network. The next chapter will show how these processes were implemented and simulated to model realistic network conditions.

# D. Protocol Transfer Notation (PTN)

| Symbol | Description |
|---|---|
| $GPS_X$ | GPS node where X is the ID of the node |
| $ID_X$ | ID of node X |
| A,B,C | Non-GPS nodes where A,B,C is the ID of the node |
| ->, <- | Direction of Communication |
| $E_{KR}[ \dots ]$ | Encryption using a private key |
| $E_{KU}[ \dots ]$ | Encryption using a public key |
| $E_{XY}[ \dots ]$ | Encryption using a shared key between x and y |
| N | A nonce or randomly generated number |
| f( … ) | A function performing mathematical operations |

**A. Initialization Process**

*1. Building neighbor list of GPS and non-GPS nodes*

| | | | Data |
|---|---|---|---|
| 1. | $GPS_1$ | -> A | Broadcast |
| 2. | A | -> $GPS_1$ | $ID_A$, N ($GPS_1$ adds A to list) |
| 3. | $GPS_1$ | -> A | $E_{KR}[ ID_A, location(x_1,y_1,z_1) ]$, f(N) (A adds $GPS_1$ to list) |

*2. Building neighbor list of GPS nodes*

| | | | |
|---|---|---|---|
| 1. | $GPS_1$ | -> $GPS_2$ | Broadcast |
| 2. | $GPS_2$ | -> $GPS_1$ | $E_{KR}[ location(x_1,y_1,z_1) ]$, N ($GPS_1$ adds $GPS_2$) |
| 3. | $GPS_1$ | -> $GPS_2$ | $E_{KR}[ location(x_1,y_1,z_1) ]$, f(N) ($GPS_2$ adds $GPS_1$) |

*3. Building neighbor list of non-GPS nodes*

| | | | |
|---|---|---|---|
| 1. | $GPS_1$ | -> A | Broadcast |
| 2. | A | -> B | $ID_A$, N (B adds A to list) |
| 3. | B | -> A | $ID_B$, f(N) (A adds B to list) |

**B. Communication Process**

*1. Communication via non-GPS nodes*

| | | | |
|---|---|---|---|
| 1. | A | -> B | $K_{AB}[ ID_A, ID_C$, A's GPS List, $K_{AC}[data]]$ , N |

2. B -> C $K_{BC}[ ID_A, ID_C, B's\ GPS\ List, K_{AC}[data]] , f(N)$

*2. Communication via GPS nodes*

1. A -> $GPS_1$ $ID_A, ID_C, A's\ GPS\ List, K_{AC}[data], N$
2. $GPS_1$ -> C $E_{KR} [ ID_A, ID_C, location(x,y,z) , K_{AC}[data]], f(N)$

Node C verifies f(N) and decrypts to receive message.

**C. Detection Process**

*1. One-Hop Calculation*

Distance of A's nearby GPS1 and GPS2 > Transmission Radius x 2

*2. Two-Hop Calculation*

Distance of A's GPS1 and B's GPS2 > Transmission Radius x 3

# Chapter 4: Experiments, Results and Discussion

The first section will talk about this project's choice of development tools. The second section will report on development of the program used to simulate the design of the protocol. After providing the details of the implementation, the third section will discuss the various experiments conducted and report their results. Based on these results, the fourth section will discuss effectiveness of this protocol to prevent wormhole attack.

## A. Choice of Development Tools

After experimenting with different development tools, I decided to use an open-source Java class library called JFreeChart (available at http://www.jfree.org/jfreechart/index.html) to implement the simulation. JFreeChart was chosen over alternative development tools such as GNUplot, PHPlot and JOpenChart because of the following criteria:

- Relatively low learning curve
- Large amount of documentation and examples
- Java-based programming
- User-friendly environment
- Detailed graphical interface

The alternative development tools were either lacking in one or more of these categories above. JFreeChart allows users to easily plot and graph data without going into detail on how to use Java graphic libraries. Because of the large amount of documentation and example files, this project can focus more on implementing the protocol design rather than learning the functions and internal workings of the library.

## B. Software Development

Using JFreeChart, I created a program that plots random coordinates on an X-Y plane as depicted in Figure 9 and simulates their behavior according to the protocol design.

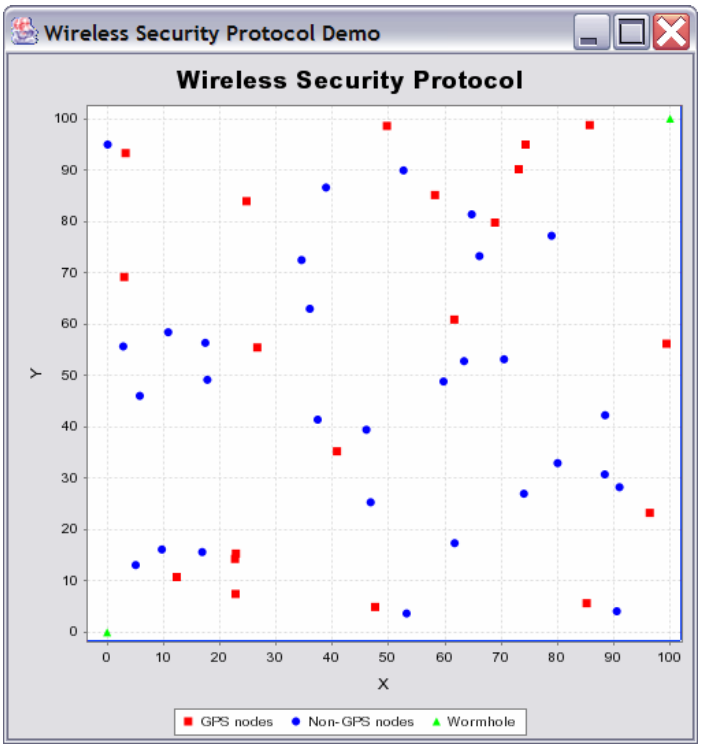


**Figure 9: JFreeChart GUI Software.** Displays GPS nodes, non-GPS nodes and the wormhole scattered randomly on an x-y plane.

The program consists of three classes: the simulation, node and graphical user interface (GUI) class. The simulation class is the most important class as it implements the design of the protocol. The number of GPS nodes, non-GPS nodes and wormholes, the location of the nodes and wormholes, their transmission radius and the size of the network area can be configured in this class. The other two classes work to support the simulation class. The node class is used primarily to hold data. Each node's actual location, perception of location due to GPS nodes and wormholes and neighbor list are

held in this class. On the other hand, the GUI class simply takes x and y coordinates from the simulation class and displays the X-Y plot graph on the screen. All three classes work together to produce results which are reported in a text file for easy access.

## C. Experiments and Results

Two experiments were conducted to verify the effectiveness of the protocol. These experiments show whether the protocol design could work on wireless networks with the following conditions:

- Limited numbers of GPS nodes
- Large network areas
- Ad-hoc or randomized networks

Highlights of the simulation results are provided in this chapter. For the complete table of results, please refer to Appendix B.

### 1. First Experiment: Limited Number of GPS Nodes

The first experiment analyzes the effectiveness of the protocol design under varying numbers of GPS nodes to non-GPS nodes. The ratios of GPS nodes to non-GPS nodes tested are 30:20, 25:25, 20:30, 15:35, 10:40 and 5:45 under a total network area of 100 by 100 meters. In this experiment, all nodes can hear any other node within a transmission radius of twenty-five meters. The wormholes are in a fixed position on the top-right and bottom-left during all stages of this experiment.

After conducting ten trials of the first experiment, the results show that lower numbers of GPS nodes relative to non-GPS nodes leads to fewer wormhole detections as shown in Figure 10.

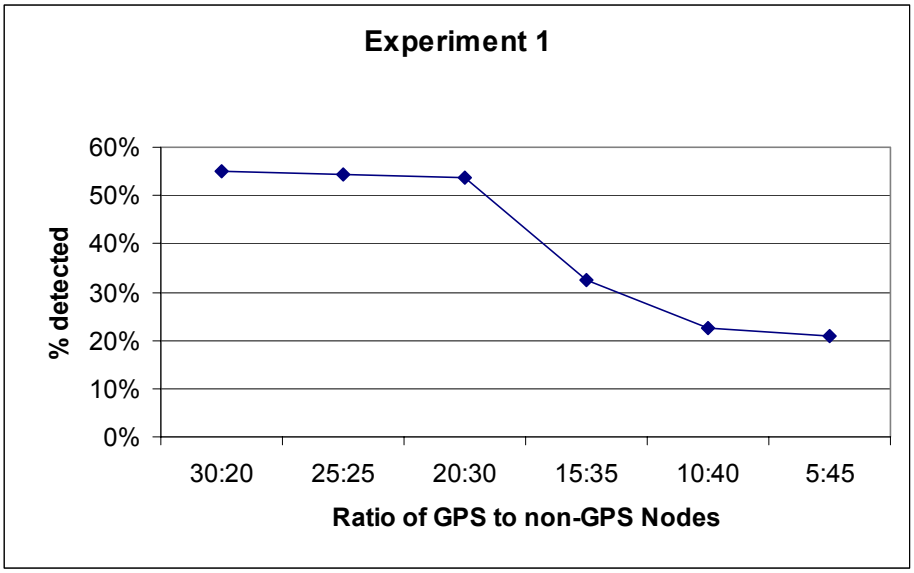


**Figure 10: Experiment 1 Results.** Shows the % of the number of nodes that detected wormholes over the number of nodes with actual wormholes within their transmission radius under varying numbers of GPS and non-GPS nodes.

The percentage shown in Figure 10 is the total number of wormhole detections divided by the total number of actual wormholes. The total number of wormhole detections is determined using the one-hop and two-hop calculations discussed in chapter three. Each GPS and non-GPS node uses its neighbor list of GPS nodes to determine whether or not it is affected by a wormhole. The total number of actual wormholes is determined by the number of nodes within the transmission radius of the wormhole. From Figure 10, the protocol can detect an average of 54-55% of the nodes affected by a wormhole in networks consisting of a 30:25, 25:25 and 20:30 GPS to non-GPS node ratio. However, when the network is introduced with only 15 GPS and 35 non-GPS nodes, the protocol detection rate reduces to 33%. The data seems to indicate that the detection rate is a linearly related until it reaches the 15:35 GPS to non-GPS ratio where it drops exponentially.

**2. Second Experiment: Density Check**

The second experiment determines whether the network will be able to detect wormholes under different densities. The density of the network is increased by adding more nodes on the network under a constant area. A 2:3 ratio of GPS to non-GPS nodes is maintained on this experiment because this ratio as proven to work as well as the higher GPS to non-GPS ratios in the first experiment. Distributions of 100, 75, 50, 30 and 20 nodes are tested in a network area of 100 by 100 meters. Ratios of 2:3 GPS to non-GPS nodes of these distributions are 40:60, 30:45, 20:30, 12:18 and 8:12 respectively. Again, the wormholes are in a fixed position on the top-right and bottom-left during all stages of this experiment.

The results on the second experiment show lower densities of nodes result in fewer wormhole detections as depicted in Figure 11. Figure 12 shows the connectivity of non-GPS nodes in different densities. Each non-GPS node must be nearby at least one GPS node to be connected to the network. Larger numbers of nodes tend to lead to better wormhole detection as well as connectivity of the network. The density of the network seems to have a linear relationship with the wormhole detection rate while it has an exponential relationship with the connectivity of nodes in the network.

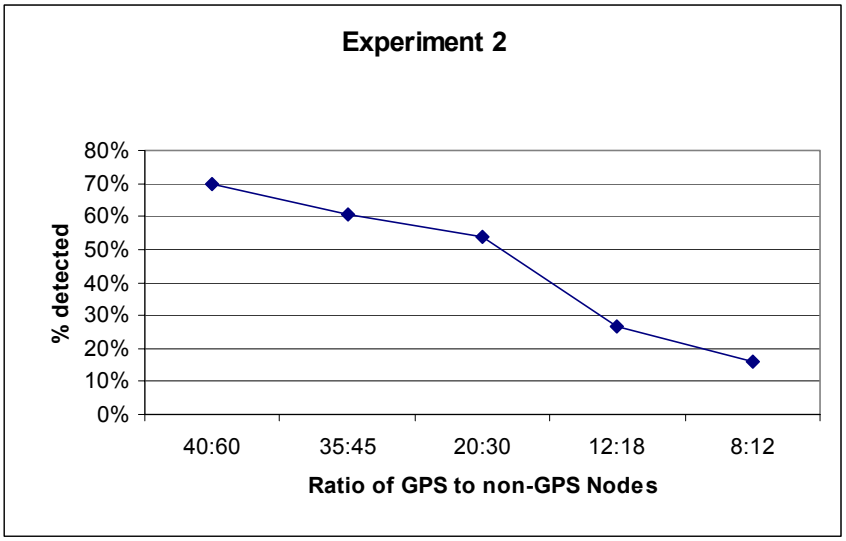


**Figure 11: Test 2 Results.** Shows the % of the number of nodes that detected wormholes over the number of nodes with actual wormholes within their transmission radius under varying densities.

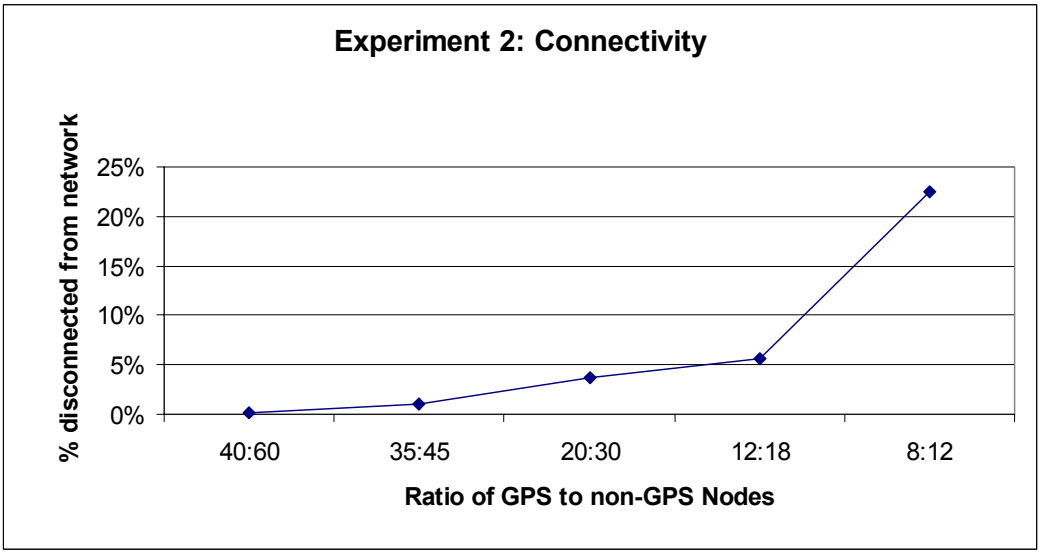


**Figure 12: Connectivity.** Shows the % of the number of non-GPS nodes that are disconnected wormholes under varying network densities.

## D. Discussion

To test how well the protocol works under ad-hoc wireless networks, ten trials of the first and second experiments were conducted. Each trial places the GPS and non-

GPS nodes in different locations. The averages of all the trials and standard deviation or variance of the data are calculated to determine if the protocol works better under different network structures.

From these experiments, it is clear that the highest percentage of total number of nodes detecting wormholes comes from a distribution of 40 GPS and 60 non-GPS nodes on a 100 x 100 meter network area. The results show that this protocol can effectively detect slightly over half of the nodes affected by a wormhole. However, in reality major users of wireless networks would not adopt this protocol as it does not provide adequate protection against wormhole attacks compared to existing protocols.

Looking more closely at the raw data, we can see that this project has a higher success rate in detecting nodes which have wormholes within one-hop than those within two-hops as shown in Figure 13 and 14. This may suggest that two-hop calculations may not be as effective as one-hop calculations in the design of this protocol. One-hop calculations and two-hop calculations are disjoint; one-hop detection of a wormhole attack exists independently of two-hop detection. Since both calculations can detect the same wormhole, the experiments conducted in this project take careful steps to avoid double-counts.

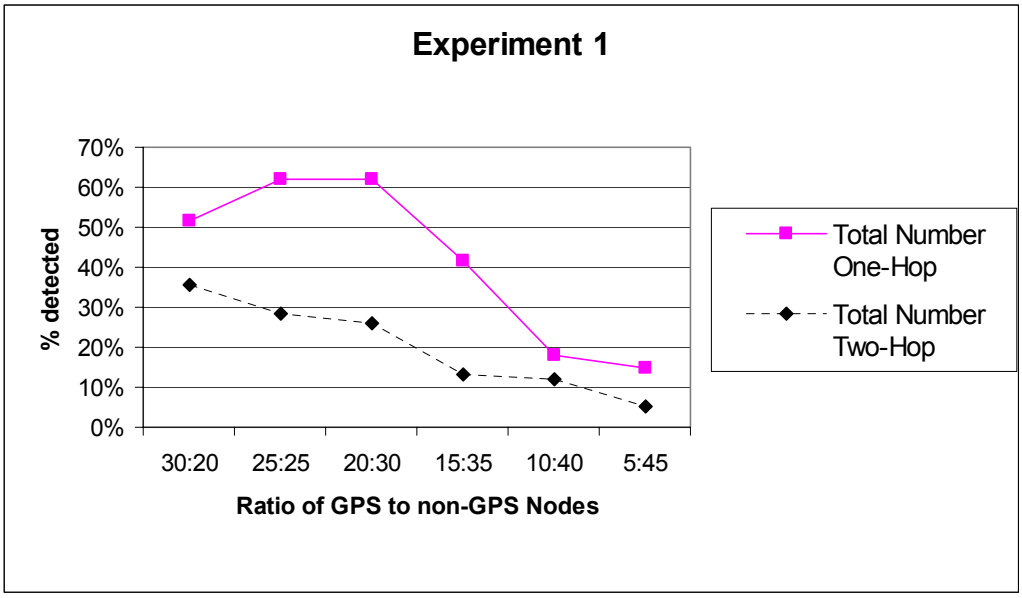


**Figure 13: Experiment 1 Results.** Shows the % of the number of nodes that detected wormholes using one-hop and two-hop calculation over the number of nodes with actual wormholes within one-hop and two-hop under varying numbers of GPS and non-GPS nodes.

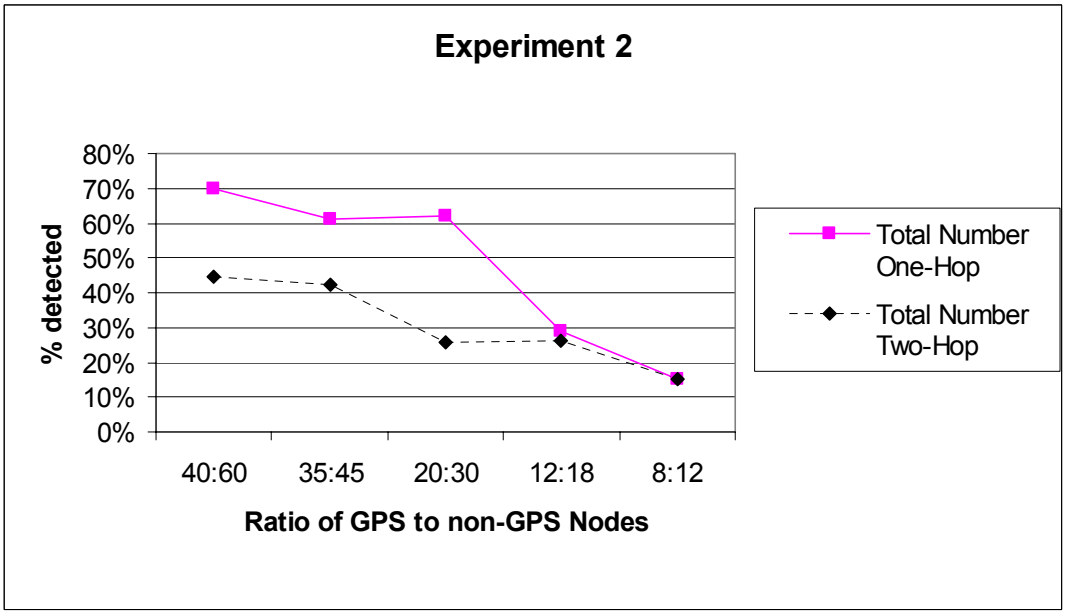


**Figure 14: Experiment 2 Results.** Shows the % of the number of nodes that detected wormholes using one-hop and two-hop calculation over the number of nodes with actual wormholes within one-hop and two-hop under varying network sizes.

A glance at the average and standard deviations in the raw data suggests that the performance of detecting wormholes depend on the structure of the network. The location of the wormhole endpoints and GPS nodes to non-GPS nodes significantly

changes the results of the data. The data between different trials in Appendix B shows that a majority of the variables are more than one standard deviation from the norm. The protocol performs the best on trial 2 while it performs the worst on trial 10 in detecting a wormhole.

# Chapter 5: Conclusion

Wormhole attacks are significant problems that need to be addressed in wireless network security. Although substantial research has been done to combat wormhole attacks, this protocol is one of the first to implement a collaboration of GPS and non-GPS nodes as an aid to prevent this type of attack. The simulation results indicate that nodes working under this protocol have the potential to detect slightly over half of the actual nodes compromised by a wormhole. This project holds confidence that further research in using GPS nodes may lead to better detection of wormholes. By having only a subset of GPS nodes, the costs of producing a secure network are significantly lower than the costs associated with the existing protocols noted in chapter two. The collaboration between GPS and non-GPS nodes has introduced a new way of preventing wormhole attacks. Users of wireless networks especially in applications of sensor networks will benefit from continued research in this form of prevention. For those who are interested pursuing work in this field of wireless network security, Appendix A provides recommendations for future work.

# Bibliography


1. Bulusu, N, J. Heidemann and D. Estrin. "GPS-less Low Cost Outdoor Localization for Very Small Devices." IEEE Personal Communications Magazine, October 2000. 23 October 2003 < www.isi.edu/~johnh/PAPERS/Bulusu00a.pdf >.

2. He, Tian, Chengdu Huang, Brain M. Blum, John A. Stankovic and Tarek Abdelzaher. "Range-Free Localization Schemes for Large Scale Sensor Networks." Mobicom 2003. 23 October 2003 < www.cs.virginia.edu/~th7c/paper/APIT_CS-2003-06.pdf >.

3. Hu, Lingxuan. "Some Security Issues in Wireless Sensor Networks." E-mail to the author. 23 October 2003.

4. Hu, Lingxuan and David Evans. "Using Directional Antennas to Prevent Wormhole Attacks." Network and Distributed System Security (NDSS 2004), February 2004.

5. Hu, Lingxuan and David Evans. "Localization for Mobile Sensor Networks." MobiCom 2004. 21 March 2004.

6. Hu, Yih-Chun, Adrian Perrig and David B. Johnson. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks." 23 October 2003. < www.monarch.cs.rice.edu/monarch-papers/tikreport.pdf >.

7. Jacques Ellul Society. "Seventy-Six Reasonable Questions to Ask About Any Technology." 23 October 2003. < http://www.newdream.org/tech/76.html >.

8. Ko, Y., V. Shankarkumar and N. H. Vaidya. "Medium access control protocols using directional antennas in ad hoc networks." Proc. Of IEEE INFOCOM, pp. 13-21, 2000. 23 October 2003 < www.ieee-infocom.org/2000/papers/350.pdf >.

9. Karlof, Chris and David Wagner. "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures." 23 October 2003 < http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf >.

10. Nagpal, Radhika, Howard Strobe and Jonathan Bachrach. "Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network." 23 October 2003 < http://www.swiss.ai.mit.edu/projects/amorphous/papers/ipsn-2003-v5.pdf >.

11. Nasipuri, A. J. Mandava, H. Manchala and R. E. Hiromoto. "On Demand Routing Using Directional Antennas in Mobile Ad Hoc Networks." Prof. of the IEEE WCNC 2000. 23 October 2003 < utsa.edu/~nasipuri/pubs/247.pdf >.

12. Niculescu, D. and B. Nath. "Ad Hoc Positioning System (APS) using AoA." INFOCOM 03, San Francisco, CA 2003. 23 October 2003 < http://paul.rutgers.edu/~dnicules/research/aps/dcs-tr-468.pdf >.
13. Pacey, Arnold. The Culture of Technology Cambridge: The MIT Press, 1985.

14. Papadimitratos, P. and Z. Haas. "Secure routing for mobile ad hoc networks." In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002. 23 October 2003 < http://wnl.ece.cornell.edu/Publications/cnds02.pdf >.

15. Perrig, Adams, Robert Szewczyk, Victor Wen, David Culler and Doug Tygar. "SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal (WINE), September 2002. 23 October 2003 < http://www.ece.cmu.edu/~adrian/projects/mc2001/spins-wine-journal.pdf >.

16. Sastry, Naveen, Umesh Shankar, and David Wagner. "Secure Verification of Location Claims." ACM Workshop on Wireless Security (WiSe 2003), September 19, 2003. 23 October 2003. < www.cs.berkeley.edu/~nks/locprove/csd-03-1245.pdf >.

17. The ETC Group. "The Big Down: Atomtech: Technologies Converging at the Nano-Scale" 23 October 2003 < http://www.etcgroup.org/documents/BigDownfinalrevisedNR.pdf >

18. "Will Big Brother Track You by Cell Phone?" PC World. September 2001. 23 October 2003 < http://www.pcworld.com/news/article/0,aid,55986,00.asp >

# Appendix A. Recommendations for Future Work

Researchers and students interested in the design of this protocol can access the source code of the simulation online at http://www.cs.virginia.edu/~jk5t/protocol.zip. This program can be compiled on any Java Integrated Development Environment (IDE) with the use of JFreeChart libraries found at http://www.jfree.org/jfreechart/index.html.

Professor David Evans and graduate student Lingxuan Hu are currently experimenting with configurations of GPS nodes and non-GPS nodes to detect wormhole attacks. A recent journal titled the "Localization for Mobile Sensor Network" has been submitted on March 15, 2004 to the MobiCom, an international forum addressing mobile computing and wireless networking. This document investigates the use of GPS to detect the relative locations of each node in a network. The findings of the document may enhance the ability of this project's protocol in detecting wormhole attacks.

# Appendix B: Simulation Results

## A. Variables

- **# detected under one-hop** - refers to the number of nodes which have detected a wormhole using the one-hop calculation mentioned in chapter 3.
- **# detected under two-hop –** similar to **# detected under one-hop** except it uses the two-hop calculation mentioned in chapter 3.
- **# actual under one-hop** - refers to the number of nodes that are within the transmission radius of the wormhole.
- **# actual under two-hop** - refers to the number of nodes which have at least one node in their neighbor list that hears a wormhole (see figure). Note that when calculating the number of actual wormholes, nodes already counted in **# actual under one-hop** do not get counted here.
- **% detected under one-hop –** a percentage determined by **# detected under one-hop** divided by **# actual under one-hop.**
- **% detected under one-hop –** same as above except it uses **# detected under two-hop** divided by **# actual under two –hop.**
- **% total under one-hop –** sum of GPS and non-GPS **# detected under one-hop** divided by **# actual under one-hop.**
- **% total under two-hop –** sum of GPS and non-GPS **# detected under two-hop** divided by **# actual under two –hop.**
- **% total detection -** sum of GPS and non-GPS **# detected under one-hop and two-hop** divided by **# actual under one-hop and two –hop.**
- **# without GPS –** refers to the non-GPS nodes which do not have a GPS node in its neighbor list.
- **% without GPS –** a percentage determined by **# without GPS** divided by the total number of non-GPS nodes.

## B. Raw Data

| Ex. 1 (30:20 GPS to non-GPS) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Avg | Std. Dev |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | |
| # detected under one hop | 3 | 6 | 2 | 2 | 0 | 0 | 0 | 0 | 5 | 0 | 1.8 | 2.25093 |
| # actual under one hop | 3 | 6 | 2 | 2 | 2 | 0 | 0 | 1 | 5 | 1 | 2.2 | 1.98886 |
| # detected under two hops | 0 | 6 | 3 | 5 | 0 | 0 | 0 | 0 | 4 | 0 | 1.8 | 2.4404 |
| # actual under two hops | 0 | 6 | 3 | 5 | 7 | 0 | 0 | 6 | 4 | 3 | 3.4 | 2.67499 |
| % detected under one hop | 100% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 40% | |
| % detected under two hops | 0% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 30% | |
| **# Non-GPS** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | |
| # without GPS | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0.3 | 0.94868 |
| % without GPS | 0% | 0% | 0% | 0% | 0% | 15% | 0% | 0% | 0% | 0% | 2% | |
| # detected under one hop | 1 | 0 | 3 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0.7 | 1.05935 |
| # actual under one hop | 1 | 0 | 3 | 0 | 4 | 4 | 2 | 1 | 2 | 2 | 1.9 | 1.44914 |
| # detected under two hops | 1 | 0 | 3 | 0 | 5 | 0 | 2 | 0 | 1 | 0 | 1.2 | 1.68655 |
| # actual under two hops | 1 | 0 | 3 | 0 | 12 | 18 | 6 | 2 | 1 | 7 | 5 | 5.94418 |
| % detected under one hop | 100% | 0% | 100% | 0% | 25% | 0% | 0% | 0% | 100% | 0% | 33% | |
| % detected under two hops | 100% | 0% | 100% | 0% | 42% | 0% | 33% | 0% | 100% | 0% | 38% | |
| % total one hop | 100% | 100% | 100% | 100% | 17% | 0% | 0% | 0% | 100% | 0% | 52% | |
| % total two hop | 100% | 100% | 100% | 100% | 26% | 0% | 33% | 0% | 100% | 0% | 36% | |
| **% total wormholes detected** | **100%** | **100%** | **100%** | **100%** | **24%** | **0%** | **25%** | **0%** | **100%** | **0%** | **55%** | |

| **Ex 1 (25:25 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | |
| # detected under one hop | 7 | 6 | 0 | 4 | 3 | 0 | 0 | 3 | 6 | 0 | 2.9 | 2.80674 |
| # actual under one hop | 7 | 6 | 4 | 4 | 3 | 2 | 2 | 3 | 6 | 1 | 3.8 | 1.98886 |
| # detected under two hops | 1 | 6 | 0 | 8 | 2 | 0 | 0 | 4 | 3 | 0 | 2.4 | 2.83627 |
| # actual under two hops | 1 | 6 | 14 | 9 | 6 | 6 | 7 | 8 | 5 | 3 | 6.5 | 3.50397 |
| % detected under one hop | 100% | 100% | 0% | 100% | 100% | 0% | 0% | 100% | 100% | 0% | 60% | |
| % detected under two hops | 100% | 100% | 0% | 89% | 33% | 0% | 0% | 50% | 60% | 0% | 43% | |
| **# Non-GPS** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | **25** | |
| # without GPS | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 2 | 0 | 0 | 0.8 | 1.39841 |
| % without GPS | 8% | 0% | 0% | 0% | 0% | 16% | 0% | 8% | 0% | 0% | 3% | |
| # detected under one hop | 2 | 3 | 2 | 3 | 5 | 0 | 1 | 3 | 3 | 0 | 2.2 | 1.54919 |
| # actual under one hop | 2 | 3 | 6 | 3 | 7 | 5 | 3 | 3 | 3 | 6 | 4.1 | 1.72884 |
| # detected under two hops | 2 | 1 | 5 | 1 | 6 | 0 | 2 | 2 | 2 | 0 | 2.1 | 1.96921 |
| # actual under two hops | 2 | 1 | 16 | 1 | 11 | 22 | 10 | 3 | 2 | 26 | 9.4 | 9.26403 |
| % detected under one hop | 100% | 100% | 33% | 100% | 71% | 0% | 33% | 100% | 100% | 0% | 64% | |
| % detected under two hops | 100% | 100% | 31% | 100% | 55% | 0% | 20% | 67% | 100% | 0% | 57% | |
| % total one hop | 100% | 100% | 20% | 100% | 80% | 0% | 20% | 100% | 100% | 0% | 62% | |
| % total two hop | 100% | 100% | 17% | 90% | 47% | 0% | 12% | 55% | 71% | 0% | 28% | |
| **% total wormholes detected** | **100%** | **100%** | **18%** | **94%** | **59%** | **0%** | **14%** | **71%** | **88%** | **0%** | **54%** | |

| **Ex 1 (20:30 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | |
| # detected under one hop | 5 | 5 | 0 | 4 | 2 | 0 | 0 | 2 | 5 | 0 | 2.3 | 2.26323 |
| # actual under one hop | 5 | 5 | 3 | 4 | 2 | 2 | 2 | 2 | 5 | 1 | 3.1 | 1.52388 |
| # detected under two hops | 0 | 5 | 0 | 6 | 1 | 0 | 0 | 3 | 2 | 0 | 1.7 | 2.26323 |
| # actual under two hops | 0 | 5 | 7 | 7 | 5 | 6 | 7 | 5 | 3 | 3 | 4.8 | 2.25093 |
| % detected under one hop | 100% | 100% | 0% | 100% | 100% | 0% | 0% | 100% | 100% | 0% | 60% | |
| % detected under two hops | 0% | 100% | 0% | 86% | 20% | 0% | 0% | 60% | 67% | 0% | 33% | |
| **# Non-GPS** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | |
| # without GPS | 2 | 0 | 0 | 0 | 0 | 5 | 0 | 4 | 0 | 0 | 1.1 | 1.91195 |
| % without GPS | 7% | 0% | 0% | 0% | 0% | 17% | 0% | 13% | 0% | 0% | 4% | |
| # detected under one hop | 4 | 4 | 2 | 3 | 6 | 0 | 1 | 4 | 4 | 0 | 2.8 | 1.98886 |
| # actual under one hop | 4 | 4 | 7 | 3 | 8 | 5 | 3 | 4 | 4 | 6 | 4.8 | 1.68655 |
| # detected under two hops | 2 | 1 | 6 | 3 | 6 | 0 | 2 | 2 | 3 | 0 | 2.5 | 2.12132 |
| # actual under two hops | 2 | 1 | 25 | 3 | 12 | 22 | 11 | 5 | 4 | 29 | 11.4 | 10.3837 |
| % detected under one hop | 100% | 100% | 29% | 100% | 75% | 0% | 33% | 100% | 100% | 0% | 64% | |
| % detected under two hops | 100% | 100% | 24% | 100% | 50% | 0% | 18% | 40% | 75% | 0% | 51% | |
| % total one hop | 100% | 100% | 20% | 100% | 80% | 0% | 20% | 100% | 100% | 0% | 62% | |
| % total two hop | 100% | 100% | 19% | 90% | 41% | 0% | 11% | 50% | 71% | 0% | 26% | |
| **% total wormholes detected** | **100%** | **100%** | **19%** | **94%** | **56%** | **0%** | **13%** | **69%** | **88%** | **0%** | **54%** | |

| **Ex. 1 (15:35 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | |
| # detected under one hop | 0 | 4 | 0 | 3 | 0 | 0 | 0 | 2 | 0 | 0 | 0.9 | 1.52388 |
| # actual under one hop | 3 | 4 | 3 | 3 | 1 | 0 | 0 | 2 | 2 | 1 | 1.9 | 1.37032 |
| # detected under two hops | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 1 | 0 | 0 | 0.9 | 1.66333 |
| # actual under two hops | 5 | 4 | 7 | 6 | 4 | 0 | 0 | 3 | 5 | 3 | 3.7 | 2.31181 |
| % detected under one hop | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 100% | 0% | 0% | 30% | |
| % detected under two hops | 0% | 100% | 0% | 67% | 0% | 0% | 0% | 33% | 0% | 0% | 20% | |
| **# Non-GPS** | **35** | **35** | **35** | **35** | **35** | **35** | **35** | **35** | **35** | **35** | **35** | |
| # without GPS | 2 | 1 | 3 | 0 | 3 | 5 | 0 | 4 | 0 | 0 | 1.8 | 1.8738 |
| % without GPS | 6% | 3% | 9% | 0% | 9% | 14% | 0% | 11% | 0% | 0% | 5% | |
| # detected under one hop | 2 | 5 | 2 | 4 | 3 | 0 | 0 | 4 | 4 | 0 | 2.4 | 1.89737 |
| # actual under one hop | 6 | 5 | 7 | 4 | 9 | 7 | 5 | 4 | 7 | 6 | 6 | 1.56347 |
| # detected under two hops | 5 | 2 | 6 | 5 | 0 | 0 | 0 | 3 | 7 | 0 | 2.8 | 2.78089 |
| # actual under two hops | 19 | 2 | 25 | 5 | 57 | 32 | 34 | 6 | 28 | 32 | 24 | 16.7597 |
| % detected under one hop | 33% | 100% | 29% | 100% | 33% | 0% | 0% | 100% | 57% | 0% | 45% | |
| % detected under two hops | 26% | 100% | 24% | 100% | 0% | 0% | 0% | 50% | 25% | 0% | 33% | |
| % total one hop | 22% | 100% | 20% | 100% | 30% | 0% | 0% | 100% | 44% | 0% | 42% | |
| % total two hop | 21% | 100% | 19% | 82% | 0% | 0% | 0% | 44% | 21% | 0% | 13% | |
| **% total wormholes detected** | **21%** | **100%** | **19%** | **89%** | **4%** | **0%** | **0%** | **67%** | **26%** | **0%** | **33%** | |

| **Ex. 1 (10:40 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | |
| # detected under one hop | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.63246 |
| # actual under one hop | 2 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0.8 | 0.78881 |
| # detected under two hops | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.3 | 0.94868 |
| # actual under two hops | 4 | 3 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 2 | 1.2 | 1.39841 |
| % detected under one hop | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| % detected under two hops | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| **# Non-GPS** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | |
| # without GPS | 8 | 9 | 7 | 6 | 12 | 12 | 1 | 18 | 6 | 8 | 8.7 | 4.54728 |
| % without GPS | 20% | 23% | 18% | 15% | 30% | 30% | 3% | 45% | 15% | 20% | 22% | |
| # detected under one hop | 0 | 4 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 0.7 | 1.33749 |
| # actual under one hop | 2 | 4 | 4 | 1 | 6 | 4 | 2 | 2 | 6 | 2 | 3.3 | 1.76698 |
| # detected under two hops | 2 | 2 | 2 | 5 | 0 | 0 | 0 | 0 | 8 | 0 | 1.9 | 2.68535 |
| # actual under two hops | 2 | 2 | 23 | 5 | 53 | 19 | 11 | 17 | 32 | 9 | 17.3 | 15.8258 |
| % detected under one hop | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 33% | 0% | 23% | |
| % detected under two hops | 100% | 100% | 9% | 100% | 0% | 0% | 0% | 0% | 25% | 0% | 33% | |
| % total one hop | 0% | 100% | 0% | 50% | 0% | 0% | 0% | 0% | 29% | 0% | 18% | |
| % total two hop | 33% | 100% | 8% | 83% | 0% | 0% | 0% | 0% | 24% | 0% | 12% | |
| **% total wormholes detected** | **20%** | **100%** | **7%** | **75%** | **0%** | **0%** | **0%** | **0%** | **25%** | **0%** | **23%** | |

| Ex. 1 (5:45 GPS to non-GPS) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Avg | Std. Dev |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **5** | **5** | **5** | **5** | **5** | **5** | **5** | **5** | **5** | **5** | **5** | |
| # detected under one hop | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.63246 |
| # actual under one hop | 2 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0.6 | 0.84327 |
| # detected under two hops | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.63246 |
| # actual under two hops | 4 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 1.31656 |
| % detected under one hop | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| % detected under two hops | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| **# Non-GPS** | **45** | **45** | **45** | **45** | **45** | **45** | **45** | **45** | **45** | **45** | **45** | |
| # without GPS | 23 | 31 | 19 | 25 | 21 | 14 | 17 | 25 | 29 | 19 | 22.3 | 5.33437 |
| % without GPS | 51% | 69% | 42% | 56% | 47% | 31% | 38% | 56% | 64% | 42% | 50% | |
| # detected under one hop | 0 | 4 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0.5 | 1.2693 |
| # actual under one hop | 2 | 4 | 4 | 1 | 6 | 4 | 2 | 2 | 7 | 3 | 3.5 | 1.90029 |
| # detected under two hops | 3 | 2 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 1.1 | 2.02485 |
| # actual under two hops | 2 | 2 | 26 | 6 | 53 | 19 | 12 | 17 | 68 | 16 | 22.1 | 21.9061 |
| % detected under one hop | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 20% | |
| % detected under two hops | 150% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 35% | |
| % total one hop | 0% | 100% | 0% | 50% | 0% | 0% | 0% | 0% | 0% | 0% | 15% | |
| % total two hop | 50% | 100% | 0% | 86% | 0% | 0% | 0% | 0% | 0% | 0% | 6% | |
| **% total wormholes detected** | **30%** | **100%** | **0%** | **78%** | **0%** | **0%** | **0%** | **0%** | **0%** | **0%** | **21%** | |

| **Ex. 2 (40:60 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | |
| # detected under one hop | 3 | 6 | 3 | 2 | 5 | 0 | 0 | 0 | 7 | 0 | 2.6 | 2.67499 |
| # actual under one hop | 3 | 6 | 3 | 2 | 5 | 3 | 0 | 1 | 7 | 1 | 3.1 | 2.28279 |
| # detected under two hops | 3 | 6 | 5 | 8 | 5 | 0 | 0 | 0 | 8 | 0 | 3.5 | 3.34166 |
| # actual under two hops | 3 | 6 | 5 | 8 | 5 | 10 | 0 | 8 | 8 | 4 | 5.7 | 2.94581 |
| % detected under one hop | 100% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 40% | |
| % detected under two hops | 100% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 40% | |
| **# Non-GPS** | **60** | **60** | **60** | **60** | **60** | **60** | **60** | **60** | **60** | **60** | **60** | |
| # without GPS | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0.1 | 0.31623 |
| % without GPS | 0% | 0% | 0% | 0% | 0% | 0% | 2% | 0% | 0% | 0% | 0% | |
| # detected under one hop | 5 | 3 | 5 | 8 | 6 | 1 | 0 | 3 | 5 | 4 | 4 | 2.35702 |
| # actual under one hop | 5 | 3 | 5 | 8 | 6 | 4 | 7 | 5 | 5 | 10 | 5.8 | 2.04396 |
| # detected under two hops | 8 | 0 | 9 | 8 | 8 | 12 | 6 | 8 | 10 | 9 | 7.8 | 3.15524 |
| # actual under two hops | 8 | 0 | 9 | 8 | 8 | 25 | 63 | 14 | 10 | 52 | 19.7 | 21.0452 |
| % detected under one hop | 100% | 100% | 100% | 100% | 100% | 25% | 0% | 60% | 100% | 40% | 73% | |
| % detected under two hops | 100% | 0% | 100% | 100% | 100% | 48% | 10% | 57% | 100% | 17% | 63% | |
| % total one hop | 100% | 100% | 100% | 100% | 100% | 14% | 0% | 50% | 100% | 36% | 70% | |
| % total two hop | 100% | 100% | 100% | 100% | 100% | 34% | 10% | 36% | 100% | 16% | 44% | |
| **% total wormholes detected** | **100%** | **100%** | **100%** | **100%** | **100%** | **31%** | **9%** | **39%** | **100%** | **19%** | **70%** | |

| **Ex. 2 (30:45 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | |
| # detected under one hop | 3 | 6 | 2 | 2 | 0 | 0 | 0 | 0 | 5 | 0 | 1.8 | 2.25093 |
| # actual under one hop | 3 | 6 | 2 | 2 | 2 | 0 | 0 | 1 | 5 | 1 | 2.2 | 1.98886 |
| # detected under two hops | 0 | 6 | 3 | 5 | 0 | 0 | 0 | 0 | 4 | 0 | 1.8 | 2.4404 |
| # actual under two hops | 0 | 6 | 3 | 5 | 7 | 0 | 0 | 6 | 4 | 3 | 3.4 | 2.67499 |
| % detected under one hop | 100% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 40% | |
| % detected under two hops | 0% | 100% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 30% | |
| **# Non-GPS** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | **40** | |
| # without GPS | 0 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 0.4 | 0.96609 |
| % without GPS | 0% | 0% | 0% | 0% | 0% | 8% | 3% | 0% | 0% | 0% | 1% | |
| # detected under one hop | 2 | 1 | 4 | 3 | 1 | 0 | 0 | 2 | 5 | 4 | 2.2 | 1.75119 |
| # actual under one hop | 2 | 1 | 4 | 3 | 6 | 5 | 3 | 3 | 5 | 7 | 3.9 | 1.85293 |
| # detected under two hops | 8 | 0 | 10 | 9 | 8 | 2 | 3 | 4 | 5 | 5 | 5.4 | 3.27278 |
| # actual under two hops | 8 | 0 | 10 | 9 | 34 | 30 | 17 | 6 | 5 | 18 | 13.7 | 11.0459 |
| % detected under one hop | 100% | 100% | 100% | 100% | 17% | 0% | 0% | 67% | 100% | 57% | 64% | |
| % detected under two hops | 100% | 0% | 100% | 33% | 24% | 7% | 18% | 67% | 100% | 28% | 48% | |
| % total one hop | 100% | 100% | 100% | 100% | 13% | 0% | 0% | 50% | 100% | 50% | 61% | |
| % total two hop | 100% | 100% | 100% | 100% | 20% | 7% | 18% | 33% | 100% | 24% | 42% | |
| **% total wormholes detected** | **100%** | **100%** | **100%** | **100%** | **18%** | **6%** | **15%** | **38%** | **100%** | **31%** | **61%** | |

| **Ex. 2 (20:30 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | |
| # detected under one hop | 5 | 5 | 0 | 4 | 2 | 0 | 0 | 2 | 5 | 0 | 2.3 | 2.26323 |
| # actual under one hop | 5 | 5 | 3 | 4 | 2 | 2 | 2 | 2 | 5 | 1 | 3.1 | 1.52388 |
| # detected under two hops | 0 | 5 | 0 | 6 | 1 | 0 | 0 | 3 | 2 | 0 | 1.7 | 2.26323 |
| # actual under two hops | 0 | 5 | 7 | 7 | 5 | 6 | 7 | 5 | 3 | 3 | 4.8 | 2.25093 |
| % detected under one hop | 100% | 100% | 0% | 100% | 100% | 0% | 0% | 100% | 100% | 0% | 60% | |
| % detected under two hops | 0% | 100% | 0% | 86% | 20% | 0% | 0% | 60% | 67% | 0% | 33% | |
| **# Non-GPS** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | |
| # without GPS | 2 | 0 | 0 | 0 | 0 | 5 | 0 | 4 | 0 | 0 | 1.1 | 1.91195 |
| % without GPS | 7% | 0% | 0% | 0% | 0% | 17% | 0% | 13% | 0% | 0% | 4% | |
| # detected under one hop | 4 | 4 | 2 | 3 | 6 | 0 | 1 | 4 | 4 | 0 | 2.8 | 1.98886 |
| # actual under one hop | 4 | 4 | 7 | 3 | 8 | 5 | 3 | 4 | 4 | 6 | 4.8 | 1.68655 |
| # detected under two hops | 2 | 1 | 6 | 3 | 6 | 0 | 2 | 2 | 3 | 0 | 2.5 | 2.12132 |
| # actual under two hops | 2 | 1 | 25 | 3 | 12 | 22 | 11 | 5 | 4 | 29 | 11.4 | 10.3837 |
| % detected under one hop | 100% | 100% | 29% | 100% | 75% | 0% | 33% | 100% | 100% | 0% | 64% | |
| % detected under two hops | 100% | 100% | 24% | 100% | 50% | 0% | 18% | 40% | 75% | 0% | 51% | |
| % total one hop | 100% | 100% | 20% | 100% | 80% | 0% | 20% | 100% | 100% | 0% | 62% | |
| % total two hop | 100% | 100% | 19% | 90% | 41% | 0% | 11% | 50% | 71% | 0% | 26% | |
| **% total wormholes detected** | **100%** | **100%** | **19%** | **94%** | **56%** | **0%** | **13%** | **69%** | **88%** | **0%** | **54%** | |

| **Ex. 2 (12:18 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | **15** | |
| # detected under one hop | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0.4 | 0.84327 |
| # actual under one hop | 2 | 2 | 1 | 2 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0.8165 |
| # detected under two hops | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 1.68655 |
| # actual under two hops | 4 | 4 | 1 | 4 | 0 | 0 | 0 | 6 | 1 | 2 | 2.2 | 2.14994 |
| % detected under one hop | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 20% | |
| % detected under two hops | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 20% | |
| **# Non-GPS** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | |
| # without GPS | 1 | 3 | 1 | 4 | 3 | 1 | 0 | 4 | 0 | 0 | 1.7 | 1.63639 |
| % without GPS | 3% | 10% | 3% | 13% | 10% | 3% | 0% | 13% | 0% | 0% | 6% | |
| # detected under one hop | 0 | 4 | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0.7 | 1.33749 |
| # actual under one hop | 1 | 4 | 1 | 0 | 2 | 0 | 0 | 1 | 4 | 0 | 1.3 | 1.56702 |
| # detected under two hops | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0.4 | 0.96609 |
| # actual under two hops | 1 | 1 | 0 | 0 | 7 | 0 | 0 | 6 | 9 | 0 | 2.4 | 3.50238 |
| % detected under one hop | 0% | 100% | 100% | 0% | 0% | 0% | 0% | 0% | 50% | 0% | 25% | |
| % detected under two hops | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 33% | 0% | 13% | |
| % total one hop | 0% | 100% | 50% | 100% | 0% | 0% | 0% | 0% | 40% | 0% | 29% | |
| % total two hop | 0% | 100% | 0% | 100% | 0% | 0% | 0% | 0% | 30% | 0% | 26% | |
| **% total wormholes detected** | **0%** | **100%** | **33%** | **100%** | **0%** | **0%** | **0%** | **0%** | **33%** | **0%** | **27%** | |

| **Ex. 2 (8:12 GPS to non-GPS)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Avg** | **Std. Dev** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **# GPS nodes** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | |
| # detected under one hop | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.63246 |
| # actual under one hop | 2 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0.7 | 0.82327 |
| # detected under two hops | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.63246 |
| # actual under two hops | 4 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 1.33333 |
| % detected under one hop | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| % detected under two hops | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | |
| **# Non-GPS** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | **20** | |
| # without GPS | 4 | 3 | 6 | 5 | 4 | 5 | 3 | 4 | 7 | 4 | 4.5 | 1.2693 |
| % without GPS | 20% | 15% | 30% | 25% | 20% | 25% | 15% | 20% | 35% | 20% | 23% | |
| # detected under one hop | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 | 0.42164 |
| # actual under one hop | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 4 | 0 | 0.9 | 1.19722 |
| # detected under two hops | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0.4 | 0.84327 |
| # actual under two hops | 1 | 2 | 0 | 2 | 3 | 0 | 0 | 4 | 17 | 0 | 2.9 | 5.15213 |
| % detected under one hop | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | |
| % detected under two hops | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | |
| % total one hop | 0% | 100% | 0% | 50% | 0% | 0% | 0% | 0% | 0% | 0% | 15% | |
| % total two hop | 0% | 100% | 0% | 67% | 0% | 0% | 0% | 0% | 0% | 0% | 15% | |
| **% total wormholes detected** | **0%** | **100%** | **0%** | **60%** | **0%** | **0%** | **0%** | **0%** | **0%** | **0%** | **16%** | |