Volume 2 Issue 1 | March 2014

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Impact of Wormhole Attacks On DV-Hop Positioning in Wireless Sensor Networks

Aparna Pandey
M. Tech. Scholar
Department of Computer Science & Engineering
Vindhya Institute of Technology and Science
Jabalpur (M.P.) [INDIA]
Email: aparnapandey29@gmail.com

Prof. Sanjay Gupta
Head of the Department
Department of Computer Science & Engineering
Vindhya Institute of Technology and Science
Jabalpur (M.P.) [INDIA]

Abstract—*This paper presents a simulation-based study of the impact of wormhole attacks on DV-Hop based positioning in wireless sensor networks. A wireless sensor grid is first simulated, the positioning of the nodes are determined using DV-Hop based positioning and then a wormhole is introduced into the grid. The effects of this wormhole on node localization for varying hop lengths between the wormhole Start Point (SP) and End Point (EP) are then determined.*

Keywords:— *DV-Hop, Start Point (SP), End Point (EP)*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are autonomous systems of tiny sensor nodes equipped with integrated sensing and data processing capabilities. These are deployed on a large-scale in resource limited and harsh environments such as seismic zones, ecological contamination sites or battlefields. The ability to acquire spatio-temporally dense data in hazardous and unstructured environments makes WSNs attractive for a wide variety of security applications. Since WSNs may be deployed in hostile environments, the nodes are subject to various forms of attacks. This makes secure routing in WSNs a very important concern.

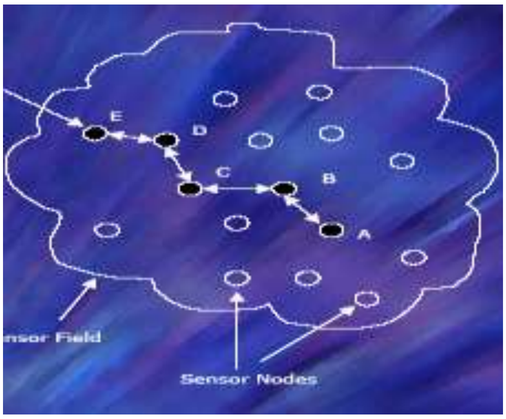

Figure.1: Wireless Sensor Network

The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. In this attack, an adversary receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. An instance of a wormhole attack would involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel (defined by the wormhole Start Point and the End Point) available only to the attacker. Thus a false route would be established which would shorten the hop distance between any two non-malicious nodes.

Wormhole attacks can cause Denial-of-Service through Data Traffic, Denial-of-Service through Routing Disruptions and

Unauthorized Access. In Denial-of-Service through Data Traffic, the malicious node(s) can insinuate itself in a route and then drop data packets. Denial-of-Service through Routing Disruptions can prevent discovery of legitimate routes and Unauthorized Access could allow access to wireless control system that are based on physical proximity, e.g. wireless car keys.

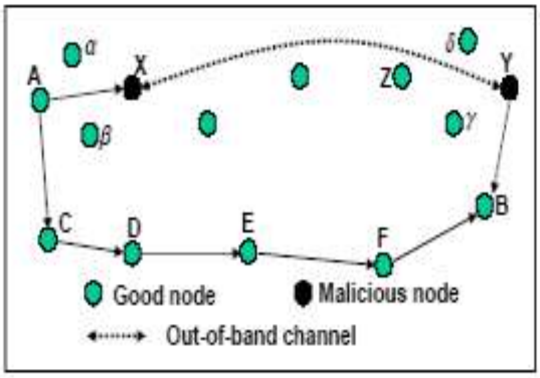

Figure 2: Wormhole Attack

The focus of this study is to determine the impact that wormholes can have on node localization for isotropic wireless sensor networks where only a limited fraction of nodes have self-positioning capability and the node positions have been determined using the "DV-hop" propagation method. The wormhole is positioned at various places on the network grid and its impact for varying hop lengths at each position is studied.

The remainder of this paper is structured as follows:

- Section 2 the background of this study is discussed.
- Section 3 describes the simulation approach;
- Section 4 discusses & analyzes the experimental evaluation study;
- Section 5 presents the related work followed by the conclusion
- Section 6.future work
- Section 7 mentions the references.

2. BACKGROUND

The nodes in WSNs are typically deployed into arbitrary topologies before organizing into a multi-hop network (using a localization algorithm) for collecting data from the environment and forwarding the data into the base station or sink. Localization is defined as the ability of the sensors in a network to determine their position in the same coordinate system.

In this study, the DV-hop propagation algorithm as proposed in [5] has been used to determine the node positions. A reduced triangulation scheme that is limited to the three closest landmarks has been adopted here.

2.1 DV-hop propagation method

This scheme envisages determining the position of any node with respect to at least three nodes called landmarks. These landmark nodes are either GPS enhanced, or know their position by some other means and are present in the WSN grid. Thus, the landmark nodes supply a convenient anchor or referencing point in the grid.

This is the most basic scheme, and it comprises of three non-overlapping stages. First, it employs a classical distance vector exchange so that all nodes in the network get distances, in hops, to the landmarks. Each node maintains a table {*Xi, Yi, hi*} and exchanges updates only with its neighbors. In the second stage, a landmark, after it cumulates distances to other landmarks, it estimates an average size for one hop, which is then deployed as a correction to the nodes in its neighborhood. When receiving the correction, an arbitrary node may then have estimate distances to landmarks, in meters, which can be used to perform the triangulation, which constitutes the third phase of the method. The correction a landmark *(Xi, Yi)* computes is a regular node gets an update from one of the landmarks, and it is usually the closest one, depending on the deployment policy and the time the correction phase of APS starts at each landmark.

$$c_i = \frac{\sum \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}}{\sum h_i}, \quad i \neq j, \text{ all landmarks } j.$$

Corrections are distributed by controlled flooding, meaning that once a node gets and forwards a correction, it will drop all the subsequent ones. This policy ensures that most nodes will receive only one correction, from the closest landmark. When networks are large, a method to reduce signaling would be to set a TTL field for propagation packets, which would limit the number of landmarks acquired by a node. Here, controlled flooding helps keeping the corrections localized in the neighborhood of the landmarks they were generated from, thus accounting for non-isotropies across the network. These correction factor values are then plugged into the triangulation procedure for a node to get an estimate position.

In DV-Hop based positioning, wormhole impacts would include incorrect calculation of the hop length between a landmark and a non-landmark node. Consequently, this would result in an incorrect calculation of the hop distance of a node from the landmark nodes, which in turn, would affect position accuracy of the nodes.

3. SIMULATION STUDY

An event-based simulator has been implemented for this study. This simulator constructs a grid-based sensor network and then calculates the node positions using DV-hop. Then a wormhole is simulated into the network. The node positions are then re-calculated using DV-hop and the differences between the first and the second calculation are determined. The wormhole position and the length are varied to determine the total no. of nodes that are impacted by this attack.

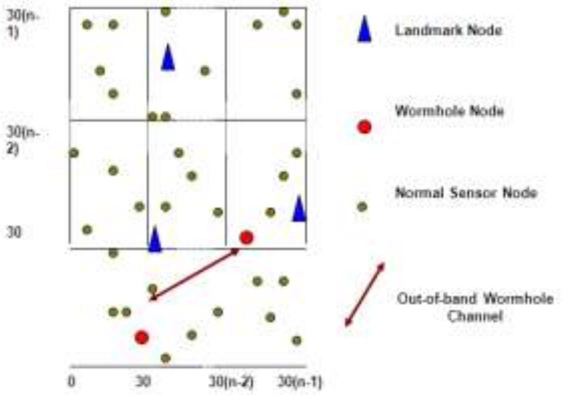

Figure 3: Sensor Network Grid Structure

3.1 Implementation of Simulator

In this study, a (n x n) grid-based sensor network has been implemented. The simulator has been implemented in C++ using STL extensively and under the LINUX operating system. An object-oriented design approach has been adopted. Use of STL has provided a great deal of flexibility to the simulator. The user specifies the following parameters:

(α) Range of the sensor nodes

(β) Size of the grid

(χ) Number of nodes per grid cell

(δ) Number of landmark nodes in the grid

(ε) Number of hops between the wormhole start and end points

A user-defined number of normal sensor nodes are then generated to populate each grid cell. The sensor nodes will be uniformly distributed in each grid cell. Depending on the range of a sensor node, all nodes that are within its immediate range are identified and are designated a neighbors of that node. The landmark nodes, as specified by the user, are then simulated and are uniformly distributed within the entire grid. At least 3 landmark nodes need to be present. The normal sensor nodes that are within the immediate range of each landmark node are then identified and are designated as immediate neighbors to that landmark. This constitutes the discovery phase of the simulator.

In the DV-hop propagation phase, each landmark node sends a “HELLO” message to all the other landmarks. The landmark node in the simulator sends the message to all the nodes within its immediate neighborhood and these nodes then propagate the message to all their immediate neighbors. This is repeated till the message reaches another landmark node. With each propagation, the number of hops is increased by one. The correction factor for each landmark node is then calculated as specified by DV-hop. All the landmark nodes then perform a distance-vector operation by sending out a “COR_FACTOR” message to the normal sensor nodes. These messages are propagated hop-by-hop till all the nodes have received this message from all the landmark nodes. As before, with every propagation, the hop number is incremented by one. Each node stores the “COR_FACTOR” message with the minimum no. of hops for each landmark and uses it to determine its position relative to 3 of the closest landmarks. These constitute the first set of readings.

In the next wormhole attack phase, a wormhole is simulated into the network. The user specifies the hop distance between the wormhole start and the end points. The distance-vector operation is again performed. The nodes then re-calculate their position relative to 3 of the closest landmarks. These constitute the second set of readings. The landmark correction factor is not affected by wormholes.

The two readings are then compared to determine the number of nodes that have been affected by the wormhole attack.

3.2 Simulation of Wormhole

In this study, the wormhole start point node is pre-determined. The user specifies the number of hops between the wormhole start and the end points. Depending on the no. of hops the end point is calculated as follows:

Initially, the start point selects from among its immediate neighbors, the node that is closest to it horizontally. This selected node then selects from its immediate neighbors, the horizontally closest node. This process is repeated for the specified number of hops and the end point node is identified. The end point node is considered to be the immediate neighbor of the start point node.

Whenever, the start point node receives a message, it transmits it only to the end point node.

4. EVALUATING IMPACT OF ATTACK

This section reports on some results from a preliminary simulation run based on the following parameters:

(α) grid size = 6

(β) range of sensor & landmark nodes = 30units

(χ) no. of nodes per grid cell = 10

(δ) no. of landmark nodes = 5

(ε) no. of hops between the wormhole start and end points = <1, 2, 3, 4, 5, 6, 7, 8>

4.1 Diagonal Wormhole start point

In the first study, the wormhole start point is repeatedly placed in the diagonal grid cells along of a section of the grid. The end points are calculated depending on the no. of hops separating the start and the end points. For each such position, the no. of hops was varied from 1 to 8. It was observed that the differing the grid positions did not have a differing impact on the number of impacted nodes for the same hop no. The impact was more dependent on the no. of hops than on the diagonal position.

Figure 4 explains the positioning of the wormhole start points along the grid diagonal. In Figure 5, the impact is presented. It is observed that the impacts of placing the start point at the diagonal grid cells are the same. For hop distances of 1 to 6, no impact is observed but for longer hop distances of 7 and 8, a significant number of nodes are impacted.

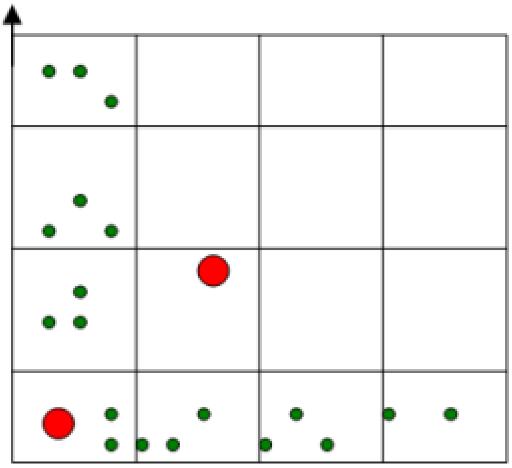

Figure 4: Wormhole at Grid Diagonal

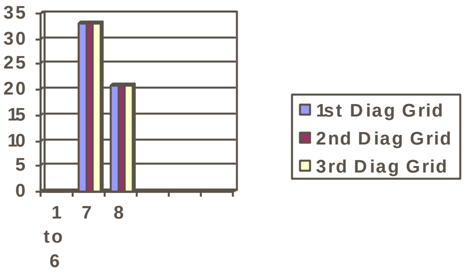

Figure 5: Impact for Wormhole at Grid Diagonal

4.2 Wormhole start point near Landmark node

In the second study, the wormhole start point was placed such that it was an immediate neighbor of a landmark node. Three simulation runs were executed by placing the start point in the immediate neighborhood of 3 different landmark nodes.

Figure 6 explains the positioning of the wormhole start point for the second study. Figure 7 presents the impact of such positioning. It is observed that impact of wormhole attack is the most when it is placed in the immediate landmark node neighborhood. As before, the lesser hop distances don't exhibit any impact and it is from hop distances of 7 & 8, that a significant number of nodes are impacted.

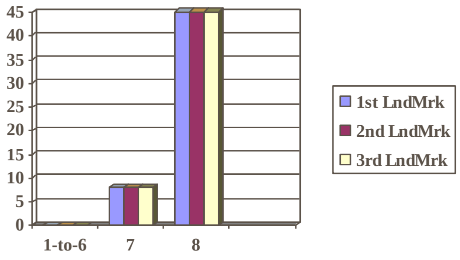

Figure 6 Wormhole at Landmark Neighborhood

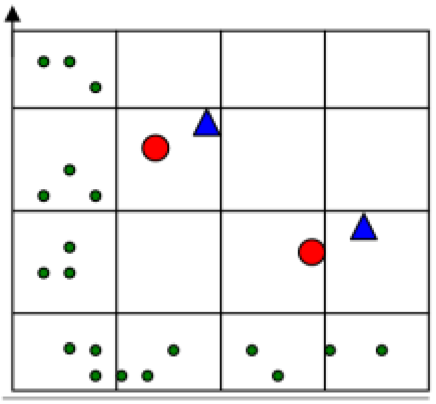

Figure 7: Impact for Wormhole at Landmark Neighborhood

5. RELATED WORK

The various types of attacks on wireless networks have been discussed in [2]. Some security mechanisms have also been discussed in [2]. The In [6], performance variation is analyzed and the after-effects of the threats to a sensor network has been measured.

6. CONCLUSION

In this study, the impact of placing wormholes at different positions in the grid and then varying the hop distance between the wormhole termination points was examined. From this study, several conclusions can be drawn. The impact of wormhole attacks is greater for greater hop distances between the wormhole start and the end points. Also, wormhole attacks are most damaging when the wormhole is an immediate neighbor of a landmark node. This is because the landmark nodes initiate the distance-vector correction and so the wormhole is in a position to inflict the maximum damage.

This work is an initial foray into the impact of wormhole attacks on grid-based sensor networks. Further work will involve studying the wormhole attack impact for grids having a dense population of sensor nodes per grid cell, greater grid sizes and with different sensor node ranges.

REFERENCES :

[1] “Security-Performance Tradeoffs of Inheritence based Key Predistribution for Wireless Sensor Networks”, Rajgopal Kannan, Lydia Ray, Arjan Durresi and S.S. Iyengar

[2] “Security in Ad hoc Networks”, Refik Molva and Pietro Michiardi

[3] https://engineering.purdue.edu/ECE/Seminars/2004-2005/01.12.2005CE.pdf

[4] “Location determination Algorithms for Distributed Wireless Sensor Networks”, Manika Sethia, Priti Mahale, Sonal Sheth

[5] “DV Based Positioning in Ad Hoc Networks”, Dragos Niculescu and BadriNath

[6] “Performance Measurement of Ad-hoc Sensor Networks under Threat (s)”, Swapnil Patil

[7] “Detection, Diagnosis, and Isolation of the Wormhole Attack in Sensor Networks”, Issa Khalil