JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

Blackhole Attacks on DV-Hop Positioning in WSN

Annavaram Kiran Kumar[1*], Dr. R. Praveen Sam[2], Dr. K. Madhavi[3]

[1*]Research Scholar, Dept Of Cse, Jntua, Anantapur-515001
[2] Professor And Head, Department Of Csbs, G Pulla Reddy Engineering College (Autonomous), Kurnool – 518007
[3]associate Professor&Hod, Dept. Of Cse, Jntucea,
Anantapur-515002

[*]**Corresponding Author Email**: Kiran.Annavaram@Gmail.Com
Emails Of Co-Authors: Rpraveensam.Cse@Gprec.Ac.In Kasamadhavi@Yahoo.Com

ABSTRACT

A simulation-based analysis of the impact of Blackhole attacks on DV-Hop based positioning in wireless sensor networks is presented in this research. A wireless sensor grid is first simulated, then the nodes' positions are established using DV-Hop based placement, followed by the introduction of a Blackhole into the grid. The impacts of this Blackhole on node localization are then determined for different hop lengths between the Blackhole Start Point (SP) and End Point (EP).

Keywords: Blackhole attack, attack positioning, DV-Hop count, Denial of Service,

1. INTRODUCTION

WSNs (Wireless Sensor Networks) are self-contained networks of small sensor nodes with integrated sensing and data processing capabilities. These are used in resource-constrained and difficult situations such as earthquake zones, ecological pollution areas, and battlefields on a huge scale. WSNs are appealing for a wide range of security applications due to their ability to capture spatiotemporally dense data in dangerous and unstructured contexts. WSN nodes are vulnerable to a variety of threats since they can be deployed in hostile situations. As a result, secure routing in WSNs is a major challenge.

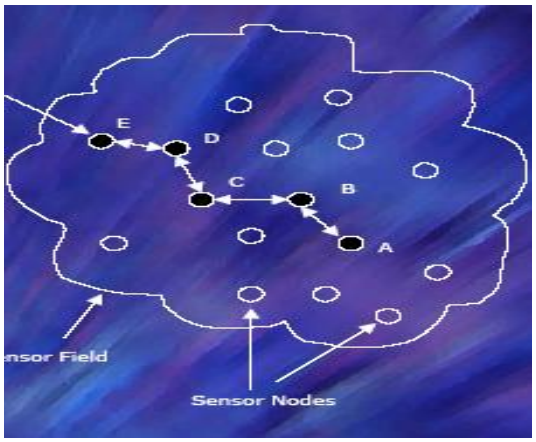

Fig. 1: Wireless Sensor Network

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

The Blackhole attack is a serious danger to sensor network packet routing that is particularly difficult to identify and mitigate. An adversary collects packets at one point in the network and tunnels them (perhaps selectively) to another point in the network, where they are resent back into the network. A Blackhole attack would include two malicious nodes working together to hide their distance from each other by relaying packets across an out-of-bound channel (specified by the Blackhole Start Point and End Point) that is only available to the attacker. As a result, a fake path would be built, reducing the hop distance between any two points.

Data traffic denial-of-service, routing disruptions denial-of-service, and unauthorised access are all examples of blackhole attacks. The malicious node(s) can infiltrate a route and subsequently drop data packets in Denial-of-Service through Data Traffic. Unauthorized Access could give access to wireless control systems that are based on physical proximity, such as wireless vehicle keys, and Denial-of-Service through Routing Disruptions could prevent legitimate routes from being discovered.

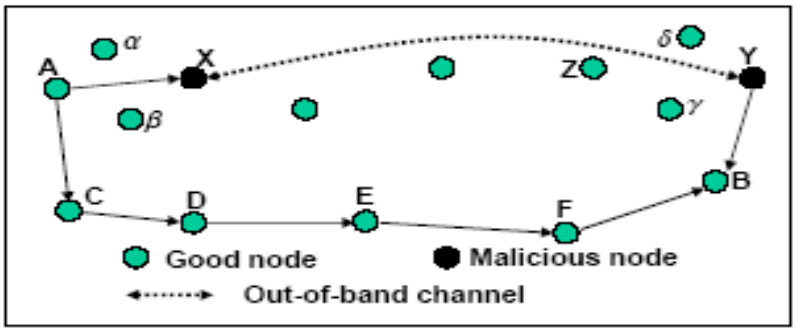

Fig. 2: Blackhole Attack

The goal of this research is to see how Blackholes affect node localization in isotropic wireless sensor networks with just a small percentage of nodes capable of self-positioning and node positions calculated using the "DV-hop" propagation method. The Blackhole is placed at several points on the network grid, and its influence is investigated for varied hop lengths at each location.

The rest of the paper is organised as follows: The study's background is explained in the following section. Section 3 explains and analyses the simulation technique; Section 4 discusses and analyses the experimental assessment study; Section 5 shows related work; and Section 6 concludes and discusses future work. The references are mentioned in Section 7.

2. BACKGROUND

WSN nodes are often deployed in various topologies before forming a multi-hop network (using a localization method) to gather data from the environment and send it to the base station or sink. The capacity of sensors in a network to establish their position in the same coordinate system is known as localization.

The DV-hop propagation technique introduced in [5] was utilized to calculate the node placements in this investigation. Here, a simplified triangulation approach based on the three closest landmarks has been used.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

2.1 DV-hop propagation method

This approach entails calculating the position of any node in relation to at least three landmarks. These landmark nodes are either GPS-enabled or have some other method of determining their location and are present in the WSN grid. As a result, the landmark nodes serve as a useful grid anchor or referring point.

This is the most basic system, and it consists of three steps that do not overlap. To begin, it uses a traditional distance vector exchange to provide distances to landmarks in hops to all nodes in the network. Each node has a table called Xi, Yi, hi and only shares updates with its neighbors. After accumulating distances to other landmarks, a landmark estimates an average hop size, which is subsequently used as a correction to the nodes in its vicinity in the second step. When an arbitrary node receives the correction, it may have estimated distances to landmarks in meters, which can be used to do the triangulation, which is the method's third phase. The adjustment computed by a landmark (Xi, Yi) is

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

Depending on the deployment policy and the time the APS correction phase begins at each landmark, a normal node receives an update from one of the landmarks, usually the closest one. Controlled flooding is used to distribute corrections, which means that if a node receives and forwards one, it will drop all subsequent ones. Because of this policy, most nodes will only receive one adjustment, from the nearest landmark. Setting a TTL field for propagation packets, which limits the number of landmarks acquired by a node, is one way to decrease signaling on big networks.

Controlled flooding aids in keeping the adjustments contained in the vicinity of the landmarks from which they were created, so correcting for network non-isotropies. These correction factor values are then used to calculate an approximate position for a node using the triangulation technique.

Blackhole affects in DV-Hop based positioning include incorrectly calculating the hop length between a landmark and a non-landmark node. As a result, the hop distance of a node from the landmark nodes will be incorrectly calculated, affecting the nodes' position accuracy.

2.2 Triangulation method

The third stage of the DV-hop propagation mechanism is this. The triangulation in this project is done using the three closest landmarks. A node's triangulated coordinates are calculated as follows:
Suppose considering node with coordinates (x,y):
(x1, y1) = coordinates of the first closest landmark
d1 = distance from first landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)

(x2, y2) = coordinates of the second closest landmark
d2 = distance from second landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)
(x3, y3) = coordinates of the third closest landmark
d3 = distance from third landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

Using the equation of a circle, the systems of equations are:

$$(x - x1)^2 + (y - y1)^2 = d1^2$$
$$(x - x2)^2 + (y - y2)^2 = d2^2$$
$$(x - x3)^2 + (y - y3)^2 = d3^2$$

Subtracting one equation from the rest:

$$2x(x2 - x1) + 2y(y2 - y1) = d1^2 - d2^2 + x2^2 - x1^2 + y2^2 - y1^2$$
$$2x(x3 - x1) + 2y(y3 - y1) = d1^2 - d3^2 + x3^2 - x1^2 + y3^2 - y1^2$$

Let $A = d1^2 - d2^2 + x2^2 - x1^2 + y2^2 - y1^2$

$B = d1^2 - d3^2 + x3^2 - x1^2 + y3^2 - y1^2$

Thus,

$$2x(x2 - x1) + 2y(y2 - y1) = A$$
$$2x(x3 - x1) + 2y(y3 - y1) = B$$

Reducing the above equations:

$$y = \frac{A(x3 - x1) - B(x2 - x1)}{2[(y2 - y1)(x3 - x1) - (y3 - y1)(x2 - x1)]}$$

$$x = \frac{[A - 2y(y2 - y1)]}{2(x2 - x1)}$$

3. Simulation Study

For this research, an event-based simulator was used. This simulator creates a grid-based sensor network and then uses DV-hop to calculate node placements. The network is then mimicked with a Blackhole. The node coordinates are then recalculated with DV-hop to find the discrepancies between the first and second calculations. To establish the overall number of nodes impacted by this attack, the Blackhole position and length are changed.

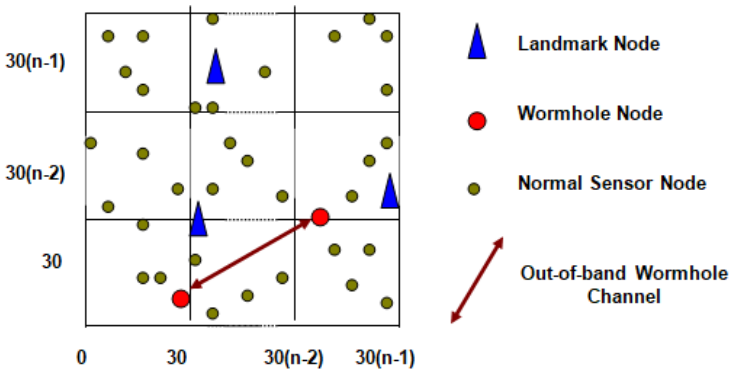

Fig. 3: Sensor Network Grid Structure

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

3.1 Implementation of Simulator

A (n × n) grid-based sensor network has been constructed in this study. The simulator was written in C++ and runs on the LINUX operating system, including a lot of STL. It was decided to use an object-oriented design strategy. The simulator's use of STL has given it a lot of versatility. The following parameters are set by the user:

a) range of the sensor nodes
b) size of the grid
c) number of nodes per grid cell
d) number of landmark nodes in the grid
e) no. of hops between the Blackhole start and end points

Each grid cell is then populated with a user-defined number of typical sensor nodes. Each grid cell will have a uniform distribution of sensor nodes. All nodes within a sensor node's immediate range are detected and assigned as neighbours of that node, depending on its range. The user-specified landmark nodes are then simulated and uniformly distributed across the entire grid. At least three landmark nodes are required. The typical sensor nodes within immediate range of each landmark node are then detected and labelled as the landmark's immediate neighbours. This is when the simulator's discovery phase begins.

Each landmark node delivers a "HELLO" message to all other landmarks during the DV-hop propagation phase. In the simulator, the landmark node sends a message to all of the nodes in its immediate vicinity, and these nodes subsequently relay the message to all of their immediate neighbors. This process is repeated until the message arrives at a new landmark node. The number of hops increases by one with each propagation. After then, the correction factor for each landmark node is determined according to DV specifications. hop's By delivering a "COR FACTOR" message to the typical sensor nodes, all of the landmark nodes do a distance-vector operation.

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.

A Blackhole is simulated into the network in the following Blackhole assault phase. The hop distance between the Blackhole start and end points is specified by the user. The distance-vector procedure is performed once more. After then, the nodes recalculate their position in relation to three of the nearest landmarks. The second batch of readings is made up of these. Blackholes have no effect on the landmark correction factor.

The number of nodes affected by the Blackhole attack is then calculated by comparing the two readings.

3.2 Simulation of Blackhole

The Blackhole start point node is pre-determined in this investigation. The number of hops between the Blackhole start and end points is specified by the user. The end point is computed as follows, depending on the number of hops:
Initially, the start point chooses the node that is horizontally nearest to it from among its immediate neighbours. This picked node then chooses the horizontally closest node from its immediate neighbours. This operation is continued until the specified number of hops has been reached, at which point the end point node is determined. The start point node's immediate neighbour is considered the end point node.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

Whenever a message is received by the start point node, it is solely sent 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:

a) grid size = 6
b) range of sensor & landmark nodes = 30units
c) no. of nodes per grid cell = 10
d) no. of landmark nodes = 5
e) no. of hops between the Blackhole start and end points = <1, 2, 3, 4, 5, 6, 7, 8>

4.1 Diagonal Blackhole start point

The Blackhole start point is repeatedly placed in the diagonal grid cells along a segment of the grid in the first study. The number of hops between the start and finish points is used to compute the end points. The number of hops was adjusted from 1 to 8 for each of these positions. It was discovered that changing the grid placements had no effect on the number of impacted nodes for the same hop node. The impact was determined by the number of hops rather than the diagonal position.

The location of the Blackhole start points along the grid diagonal is depicted in Fig. 4. The impact is depicted in Fig. 5. It has been discovered that the effects of starting at the diagonal grid cells are the same. There is no impact for hop distances of 1 to 6, but a considerable number of nodes are impacted for hop distances of 7 and 8.

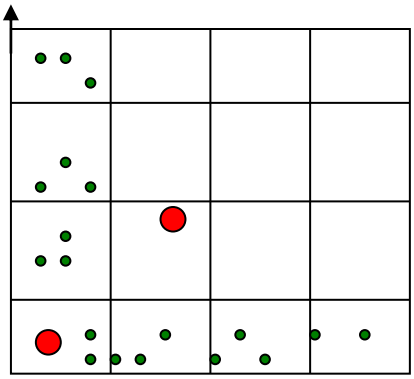

Fig. 4 Wormhole at Grid Diagonal

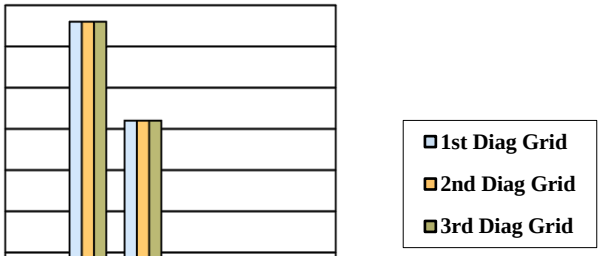

Fig. 5: Impact for Wormhole at Grid Diagonal

4.2 Blackhole start point near Landmark node

In the second experiment, the Blackhole start point was set so that it was right next to a landmark node. Three simulation runs were carried out by starting the simulation in the vicinity of three separate landmark nodes.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 421-428
https://publishoa.com
ISSN: 1309-3452

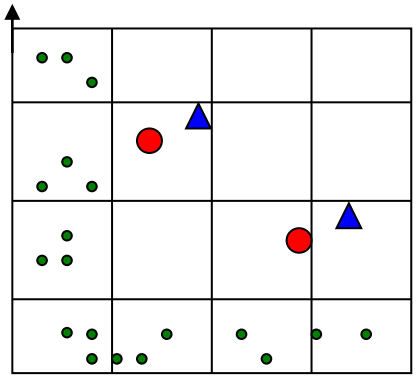

Fig. 6 Wormhole at Landmark Neighborhood

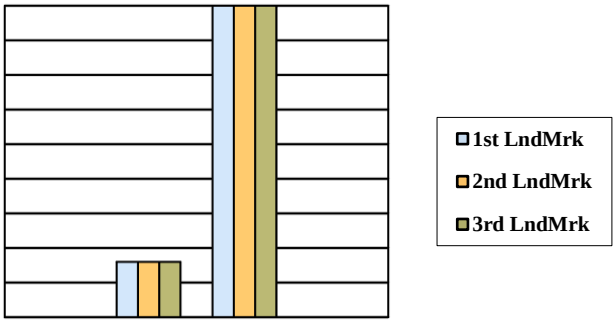

Fig. 7: Impact for Wormhole at Landmark Neighborhood

The location of the Blackhole start point for the second investigation is shown in Fig. 6. The impact of such placing is depicted in Fig. 7. It has been discovered that when a Blackhole attack is launched in the immediate vicinity of a landmark node, it has the most impact. The shorter hop distances have little effect, and it is only at hop distances of 7 and 8 that a considerable number of nodes are impacted..

5. Related Work

[2], [7] have discussed the numerous types of wireless network assaults. In [2,] some security techniques are also mentioned. The The effects of threats to a sensor network are evaluated and performance variance is analysed in [6].

6. Conclusion

The effect of installing Blackholes at various spots in the grid and then altering the hop distance between the Blackhole termination points was investigated in this study. Several conclusions can be derived from this research. Blackhole attacks have a higher impact when the hop distance between the Blackhole start and end places is greater. Also, when a Blackhole is a close neighbour of a landmark node, the attack is more devastating. This is because the landmark nodes commence the distance-vector adjustment, allowing the Blackhole to deal the most damage possible..

This research is a first look at how Blackhole attacks affect grid-based sensor networks. More research will be done on the impact of a Blackhole attack on grids with a dense population of sensor nodes per grid cell, larger grid sizes, and diverse sensor node ranges.

7. References

[1] Kalkha, Hanane, Hassan Satori, and Khalid Satori. "Preventing black hole attack in wireless sensor network using HMM." Procedia computer science 148 (2019): 552-561.

[2] Ali, Sara. "An Enhanced Virtual Private Network Authenticated Ad Hoc On-Demand Distance Vector Routing." Advances in Decision Sciences, Image Processing, Security and Computer Vision. Springer, Cham, 2020. 190-197.

[3] Ali, Sara. "An Enhanced Virtual Private Network Authenticated Ad Hoc On-Demand Distance Vector Routing." Advances in Decision Sciences, Image Processing, Security and Computer Vision. Springer, Cham, 2020. 190-197.

[4] Pawar, Mohandas V., and J. Anuradha. "Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM." International Journal of Pervasive Computing and Communications (2021).

[5] Sathyaraj, P., and K. Kannan. "Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs." (2021).

[6] Kannan, K. "Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs."

[7] Kalkha, Hanane, Hassan Satori, and Khalid Satori. "Preventing black hole attack in wireless sensor network using HMM." Procedia computer science 148 (2019): 552-561.

[8] Ahmad, Bilal, et al. "Hybrid anomaly detection by using clustering for wireless sensor network." Wireless Personal Communications 106.4 (2019): 1841-1853.

[9] Ndajah, Peter, Abdoul Ousmane Matine, and Mahouton Norbert Hounkonnou. "Black hole attack prevention in wireless peer-to-peer networks: a new strategy." International Journal of Wireless Information Networks 26.1 (2019): 48-60.

[10] Jamal, Tauseef, and Shariq Aziz Butt. "Malicious node analysis in MANETS." International Journal of Information Technology 11.4 (2019): 859-867.

[11] Subburaj, V., and K. Chitra. "Multi hop secure adhoc network to eradicate cooperative diversity." Indian Journal of Science and Technology 7.2 (2014): 135.

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

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

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

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

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

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