DETECTION AND PREVENTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORKS

1st Mr. Vishnu K
PG Scholar
Rathinam College of Arts and Science;
Coimbatore, India
k201vishnu@gmail.com

2nd Dr. Rakesh Sivalingam
Assistant Professor
Nitte Institute of Professional Education, Nitte University;
Mangaluru, India
rakesh.s@nitte.edu.in

3rd Dr. Sivaprakash
Mentor IT
iNurture Education Solutions
Coimbatore, India
p.sivaprakash@inurture.co.in

4rd Mr. Sakthi Agathiya P K
PG Scholar
Rathinam College of Arts and Science
Coimbatore, India
sakthiagathiyapk@gmail.com

5th Mr. Dinesh kumar C
PG Scholar
Rathinam College of Arts and Science
Coimbatore, India
dineshkarthi196@gmail.com

***Abstract*—A fundamental problem when transmitting a significant message via a wireless connection in a wireless sensor network (WSN). Attackers can use this to get into the network and launch a few possible attacks to intercept or change actual data. As a result of network sensors' lack of routers, every node that is part of the network must use the same routing protocol to facilitate the transmission of packets. It presents some security challenges in compounded topology, where its unguided existence frequently leaves it vulnerable to attacks against protection, especially when unguided. The wormhole is a well known example of an attack that poses the most significant risk due to the difficulty in finding and stopping it. In this paper, a brand-new routing technique that aims to provide a secure path for data transmission is presented. Wormhole attacks are taken into consideration in research, and the method used to do so aims to find and stop attacks of the type that have been identified. The suggested procedure is validated using specific performance-related WSN parameters. The generated results are evaluated based on metrics such as energy efficiency, end-to-end delay, and packet delivery ratio. These results are then compared to those of other recent techniques in the same field, and it has been determined that the exhibited research is the most effective among the methods mentioned for the parameters under consideration.**

***Index Terms*—Index Terms— AOMDV, WSN, Cluster, LNCA, Detect, Prevent, Malicious Node.**

I. Introduction

In the WSN, a number of sensor nodes are used to monitor large geographic regions, and they are designed with features such as low bandwidth, storage, and power usage to support environmentally friendly forecasting technologies. Sensor nodes collect data and are distributed to WSNs in different regions. When used within a WSN, sensor nodes can process signals, sync data with the base station, and verify routes using a minimum number of resources. Wireless sensor networks are thought to be helpful in various settings, including control over the environment, defense and military applications, deployment of robotics, and many more. WSNs are now vulnerable to various assaults as a result. These threats are alleged to involve a wormhole attack, which is a type of denial-of-service attack that utilizes both in-band and out-of-band networks. Wormhole attacks are classified as harmful attacks in a wormhole link or tunnel is a type of connection in which malicious and attacker nodes are interconnected through a fast channel connection speed. Wormhole attacks involve at least two malicious nodes, also known as attackers. The attackers take control of the network to access the data, and intruders are able to monitor wireless activity. In Mobile Ad-hoc Networks (MANETs), all nodes are mobile and able to move, but because WSN nodes have a fix protection issue for mobile, Ad-hoc networks are still useful. [1–4]. Network security is complex, while the sensor nodes mobilize their locations. In a MANET, a node is a device that communicates with other nodes without the use of a central base and often serves as a point of communication between nodes. These medium nodes function similarly to multi-hop radio networks when used with routers connected wirelessly and ad-hoc networks do not require pre-existing networking infrastructures in order to function.

II. Existing System

WSN clustering is essential to minimize energy usage and maintain the consistency of the device. Clustering is a well known and widely used technique in wireless sensor networks. Clustering is currently being implemented over a distributed approach to address problems such as network lifetime and resource availability. Clustering into sensor nodes is crucial to addressing many issues, including those with sensor networks' lifetime, scalability, and energy consumption.Algorithms that cluster data limit connectivity within domains and only send necessary data to the rest of the system via forwarding. A cluster consists of many nodes, and the local communication among the nodes are measured by the cluster's head (CH). The set typically interacts with its participant cluster to gather data. The cluster heads form one more layer of groups between themselves before they reach the drain [7,8]. The implementation of a cluster-based architecture requires extensive work. The benefits of clustering are numerous, but sensor networks also have their restrictions, issues, or challenges. In this section, we discuss some specific design and deployment issues that were addressed in the development of the network architecture based on clusters.

A. Node Mobility:

Nodes in the network are often assumed to be stationary when the network is designed. However, frequently it becomes necessary to advertise the adaptability of base stations or CHs.As a result of node mobility, clustering is observed to be more complex because node membership can change dynamically [9].

B. Traffic Load:

Sensors monitoring events can either be intermittent or persistent. Traffic will increase due to regular and continuous monitoring and tracking, which generates traffic when the relevant incident is observed. Events that occur intermittently forthe CH chosen from the sensor's population require. Loading of cluster members in an irregular manner and rotation of cluster member's position. However, intermittent events do not require periodic sensing, so the CH is not affected.

C. Overlapping Clusters:

CH may have been pre-designed by the network's designer or selected by its sensors. If the eventual option is chosen,it is likely that one cluster member will join another CH. Cluster overlapping in architecture problems must also be considered. For optimal organization between groups, detecting overlapping clusters in order to develop the perfect structures is crucial to avoid gridlock, hunger, or unfairness during the competition for resources. [10].

D. Load Balancing:

It is crucial to balance the placement of sensors in sensor networks. Sensor nodes need to be distributed evenly among the available CHs, as malfunctioning CHs may overwhelm others and cause the S. Singh, H. S. Saini 1 3head loss. Creating equal-sized clusters in these situations is crucial fora good balance.

E. Dynamic Cluster Control:

A node of a grouping device that is self-configured is required. Initial clusters are created by clustering processes and need to confirm their surroundings. They are produced based on various metrics, including the data's usefulness, nodes' capabilities, network bandwidth, etc. A significant challenge for any clustering Programme is the requirement that the cluster members evaluate each node's contribution as the process progresses. According to [10], The CH should be selected in a new round of head elections when the target is outside its sensing range.

F. Inter-cluster Coordination:

To achieve the desired outcome, CHs needed to connect. Toexchange knowledge and work as a team, they must cooperate.A different cluster head or base station in the network can request additional data collected by one cluster. The self-configuring grouping process must be able to accommodate coordination overheads between groups.

G. Data Aggregation:

The cluster head must aggregate or transfer data from cluster nodes to the CH, which requires more resources.Therefore, due diligence should be exercised when deciding on the CH. Switching positions between various nodes regularly makes it possible to maintain the CH's energy. Another option is to obtain an effective node that can handle the additional energy requirement as the CH.

H. Failure tolerance:

Failure tolerance can maintain uninterrupted sensor network functionality in the face of sensor node faults. Some sensor nodes may fail or become blocked as a result of power outages, physical harm, or environmental interference.Possible failed nodes include a CH or a piece of the cluster. Such failures shouldn't impact the overall mission or analyzing sensor performance network. Therefore, having a system that can react to these types of errors is crucial

I. Scalability:

The number of member clusters in a cluster that was initially created should be changeable by CH, either increasing or decreasing. The membership of a group can fluctuate fora variety of reasons. An environmental threat, for instance, could cause a cluster participant to fail. During this time, the CH can react to a drop in membership. Instead, under certain circumstances, the number of participants may increase in search of new nodes installation, the present CH may malfunction, etc. There must be consent from the sensor network. The number of clusters should be increased or decreased.

J. Number of Clusters:

Cluster numbering, or the total number of clusters, is a crucial architecture problem that needs to be resolved. To maintain overhead control and minimise network complexity, the cluster count must be at its maximum. To create an energy-efficient network, the ideal number of clusters would be built.

K. Cluster Formation Time:

The network's initial clustering time should be brief. Events like selecting the cluster count option, gathering CHs, and assigning cluster members to a CH should be completed as soon as possible.

L. Single hop vs Multi hops Network:

Multiple-hop communication can be used in clustering as well as single-hop communication. Because transmitting energy varies by square size, a multi-hop network is also ideal for energy conservation. [11]. The Multi-Hop Network presents architectural issues with topology management and media access control.

M. Node Heterogeneity:

Some sensor applications require deploying a complex mixture of different types and capabilities of sensor nodes. Networks may be subject to a variety of service quality constraints and follow a variety of data reporting models. Various sensors can produce data at varying rates. The heterogeneous model would be unable to cluster, making CH's task more difficult.

N. Cluster Formation:

When forming the cluster, many factors must be taken into consideration, such as whether it will be centralized or decentralized, how many groups will be included, and more. Topics such with sensor network architecture can be resolved by routing protocols that Centre on clusters. Unexpectedly, every sensor in a group is now the cluster head, dividing the energy load equally among the sensors. A network's predetermined CH allocation is made by the builder.

O. Self-Configuration and Reconfiguration:

One of the primary phases of cluster development is the self-organization process. Clusters ought to be able to adapt automatically to their environment. The ease with which the network can self-organize concerning the functional unit ispart of the wireless sensor network's main drawbacks. Tomaximize network lifetime, self-organizing process is expected to be energy efficient and reconfiguration or replenishment. The self-organization mechanism is reconfigured. when new sensor nodes are added or removed [12].

III. Challenges in Existing System

Networks become vulnerable to wormhole attacks; it receives data packets without knowing their source, draining the node's power and interfering with packet delivery. Additionally,processing received packages to a node that has never been included in the network, the wormhole in the network impacts the WSN's overall performance. The system that can anticipate the wormhole path avoids the crucial need, and a hole-free route for data transmission is projected after studying the literature on wormhole assault detection and the clustered WSN. By creating wormholes in the network, packets are received without knowing where they hail from, consuming energy and interfering with packet delivery.WSNs suffer from performance problems caused by packages sent to non-WSN nodes that have never been included in the network. It is crucial to think of the system in a way that can predict the wormholes in the path and the hole-free path for data transmission.

IV. Literature Survey

Simulation results refer to the common EEHRCP that focuses on the wormhole, whereas the proposed EEHRCP targets the wormhole. The wormhole attacks employ the round path length and have been added to the EEHRCP algorithm, and the simulation results refer to the common EEHRCP that targets the wormhole. According to the simulated results, performance can be increased by[26]. The authors used distributed trust models to isolate the misbehaving nodes. Routing has been successful using a multi-facet routing scheme. The authors improved the energy effectiveness of the network. According to Mehetre et al., a trust-based routing method might be used to ensure secure routing by using encryption. [27]. A two-stage security system was used to secure the data packet at the node selected by the authors. A cuckoo search algorithm was used to choose stable routing routes. Based on the activation function, [28] suggested a reliable set of neighbors. The purpose of this plan was to increase network security. Based on energy restrictions, the authors evaluated the significance of confidence. An additive measure was used to estimate the node, preserving the reliability of nearby nodes as well for WSNs, Deepa and Latha [29]. A hierarchical secure routing protocol was proposed by him in a hybrid routing protocol focused on clusters. Selecting the coordinator's head uses an algorithm that considers a different hierarchical group. Using an algorithm to define negative nodes, the authors selected the coordinator's head or coordinating node. When danger nodes were detected, the data was transmitted along the shortest path. Energy-aware systems based on trust were proposed by Zahedi and Parma [30]. The authors enhanced the routing functions metrics by including the node'sindirect and absolute confidence values also the energy conservation issue. The authors distinguish between the malicious nodes and the regular nodes using the measured confidence values. Mohajeran and Gharavian [31] proposed a routing method derived from the imaginative optimization of an ant colony. The writers of WSN wanted the network to last longer. With this approach, the authors achieved balanced transmission, further enhancing the energy efficiency route. In their proposal to identify malicious nodes using a multi-attribute trust protocol, Ram Prabha and Latha [32] Yurong Xu proposes that neighboring nodes detect distributed wormhole attacks based on the number of leaps determined by the node by analyzing the importance of trust with measurements like accuracy, node elapsed time, and development in messages, etc. The quickest method is to build an auxiliary graph in that case. Local map deformation is set up in an attempt to identify the wormhole hazard. Define the black hole relation using the diameter feature. The wormhole pinpoints the threat automatically when the diameter of the network reaches a certain level. The simulation's conclusion indicates that the suggested technique's identification rate is only about 80% and is not very accurate [33]. In response to Rupinder Singh's hybrid wormhole detection model, a packet is used for every hope, drop, and delay. After estimating the node's packet loss probability using the deteriorating chance of existence, which is calculated concurrently with path discovery, a probability of packet damage is calculated for the entire route. The type of attack through a wormhole is determined using these likelihood criteria [34]. Every node preserves information with the aid of the routing method protocol for almost every one of its neighboring nodes as part of the defence against wormhole assault, according to the suggestion by Parmar Amish et al. If the route information cannot be identified, the node drives a response packet while waiting for a response. Routing table is developed with the current route map, a target node determines a path that takes the same direction to reply to the sender of the data packets. If the sender receives multiple answer packets, it recognizes them:" Out there, there are many roads."When the round period (RTT) is less than the limit, the sender node defines a wormhole attack, estimates and compares the RTT to the limit, and drops specific routes [35]. A wormhole discovery approach using a critical methodology and packet leash was established by Mousam A. Patel et al. A promising method involves a watchdog node that continuously monitors the network, inspects packets submitted by a source, and then forwards them while covertly monitoring their transit. to assist the sender node in locating wormholes in the network environment, packet straps need to be aware of the node's spatial orientation and the node's way [36].

V. Methods and Proposed System

A. LNCA Outline

Phase I: Make a cluster where each step is finished throughout the study of a specific period

Step 1: Readings obtained from data interchange.

- Information is collected from the site by each node.
- Notifies its nearby neighbors of the information. In return, the same node party sends data, which the node collects.
- A node evaluates its reading in relation to the receiving node when it has access to information from its immediate neighbours. When the measurements are comparable, the transmitting node increases the "degree of node" by one.
- The transmitting node id is kept in the neighbour node list by the receiving node.

Step 2: Graduation Node Exchange.

Each node informs the neighbours in its immediate area of its "remaining energy" and "node degree". In return, the node collects the data sent to the nodes in a group that is similar to itself. In the list of adjacent nodes, each node's" node degree" matches that of the divisions. As the cluster's representative, the node chooses itself. When a node chooses a CL as the cluster head, it has higher residual energy in G and shares its degree with the nearby node population (let's say group G) ifit has the most significant degree of nodes (CH). Nearby nodes have the same residual power or full node degree if a tieis resolved by a node ID group. When a node has the lowest node ID, for instance, the cluster leader chooses itself. **Step 3:** Statement from the cluster head.

- Announcements were sent by the cluster heads (CH) chosen for their local neighbours in Stage 2. In CH announcements, the TTL3 is set to a large number.
- If the "neighbouring node list" of the cluster head node contains the final hop node from which the package was created, the cluster head node receives the CH post.Node tests Receiving node: If the acquired CH note's TTL is reduced by one if the last-hop node is found in its listof nearby nodes. If the TTL is less than zero, the node broadcasts the CH notification to its neighbours. Theparameter "received" 4 has been verified
- If "Cluster - head Received" is set to false, the source node—a root node that generated the Cluster - head notice—is declared the cluster head, and "Cluster - head Received" is set to true. Messages the cluster header to finish the "registration" process. 5 If "Cluster - head Received" at a node's endings for Step 3 is still "wrong," that node should be chosen as a "directed cluster head," rather than a Cluster - head.

Step 4: Cluster formation in the end:

In the event that a cluster is produced, the Cluster- Head adds the provided node ID to the "member node list" and receives a "registration" request.

B. Proposed System

This section discusses the recommended wormhole detection algorithm. The CH (Cluster Head) performs a crucial role inner the network. The two-layered approach is utilized to lessen the CH node's load. Every node of a sensor is distributed randomly within the ocean. The sensor nodes' job is to detect and convert the data to CH. The CH aggregates all the data it collects, which is subsequently sent to buoys on the ocean floor. The buoy on the ocean floor communicates with the base stations that analyse the detected data. LNCA is a possibility for cluster formation. The following might be used to explain LNCA clustering. A cluster head election process is achieved by randomly deployed nodes, regardless of size. Each node transmits a physical value to the number it is closestto. Node degree computation is the process of calculating all numbers of nearby neighbors. Sensor nodes with the highest node degree are designated as cluster heads.

C. System Architecture

We propose a specific method for the detection of the wormhole attack in the clustered network. Sensor nodes are immediately established, or various routes from the source to the AOMDV routing protocol are used to construct destinations. LNCA is one of the research methodologies that is frequently used to cluster the nodes for which similarity between the nodes is considered to be a significant concern. Additionally, at the initial phase of the node's deployment, cluster formation is taken into consideration. The routing protocols table contains information such as RTT, ETD, Th, P Sent, P Received, etc., which is calculated using the hop countand some initializations. Each node in a cluster needs accessto this information. The system architecture shows how the method operates in stages as it looks for network wormholes.

D. Steps of Proposed Technique

Step 1: Organization of nodes; LNCA technique used for cluster formation.

Step 2: K numbers of paths are generated in accordancewith the AOMDV routing protocol.

Step 3: When the tp1 timer is triggered, a DP (Detection Packet) is sent from S to D

Step 4: P Sent is equal to P Sent plus 1.

Step 5: After receiving an assessment packet from D, S ends the timer by computing. To determine ETD, subtract tp1 from tp2.

Step 6: Each node maintains an estimate of the parameters such as RTT, ETD, Th, P Sent, and P Received in the routing protocol table.

Step 7: A timer td1 will be set once the link is established, and S will begin sending packets of data. The process starts at td2 and ends at that time, assuming the FP is received there.

Step 8: RTT is calculated as td2 minus td1.

Step 9: A RTT will occur if: the ETD follows.

Step 10: Then CH Using this formula, P = P Sent(S, D) -P Received(S, D).

Step 11: By dividing the average RTT by the total number of leaps, a threshold is determined.

Step 12: It follows that if P ¿ Th

Step 13: Alert CH to any malicious behaviour

Step 14: CH advises S to take the alternate route by joining D and for going that path

Step 15: End.

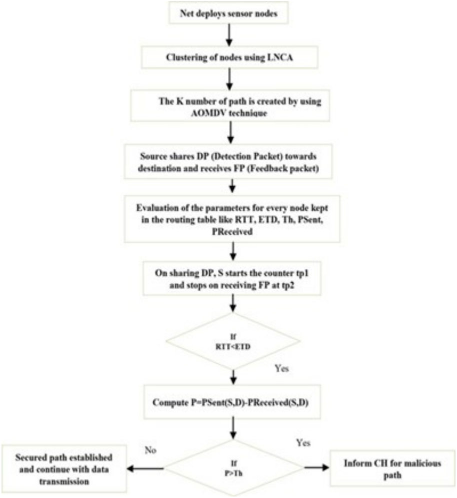
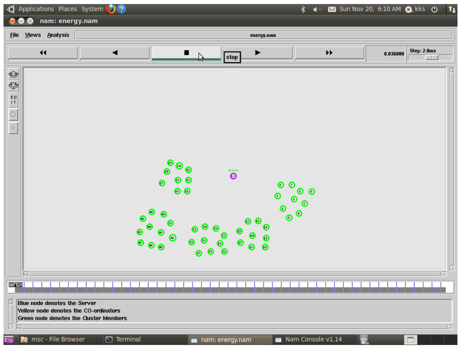

Net deploys sensor nodes
Clustering of nodes using LNCA
The K number of path is created by using AOMDV technique
Source shares DP (Detection Packet) towards destination and receives FP (Feedback packet)
Evaluation of the parameters for every node kept in the routing table like RTT, ETD, Th, PSent, PReceived
On sharing DP, S starts the counter tp1 and stops on receiving FP at tp2
If RTT<ETD
Yes
Compute P=PSent(S,D)-PReceived(S,D)
No
If P>Th
Yes
Secured path established and continue with data transmission
Inform CH for malicious path

Fig. 1. Working architecture of the research methodology

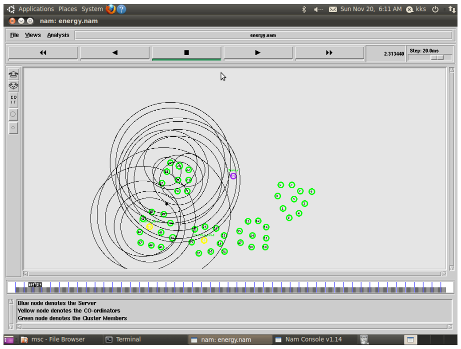
VI. Results and Discussions

It predicts the hole-free data transmission method based on the path's wormhole. the network is vulnerable to wormhole attacks; it receives data packets without knowing the source, draining the node's energy and interfering with packet delivery. Receiving packets are forwarded by the network wormhole to an outside node that has never joined the network, affecting the WSN's overall performance. In clustered WSNs, an essential requirement is to consider the literature just like that to avoid wormhole attacks. Using the wormhole present on the path, it forecasts the hole-free path for data packet transmission. Figures depict network formation following. The research methodology was simulated in NS2. The graphs represent the transmission of data between nodes orfrom a CH to lower-level nodes. Two different communication paths are shown in Fig. 5 and 6, and in Fig. According tothe methodology, the 1red line shows where a wormhole is located. As shown in Fig. 13, the packet considers path two after detecting a malicious or wormhole-containing direction. The blue line represents data transmission.



Blue node denotes the Server
Yellow node denotes the CO-ordinators
Green node denotes the Cluster Members

Fig. 2. Research methodology working architecture



Blue node denotes the Server
Yellow node denotes the CO-ordinators
Green node denotes the Cluster Members

Fig. 3. CH Invention

Energy Consumption:

Prior to choosing the best path, each free-path attacker's total energy must be calculated. In addition, the total energy in the attacker's free direction is calculated by adding theenergy levels at all intermediate nodes. This can be examined as.

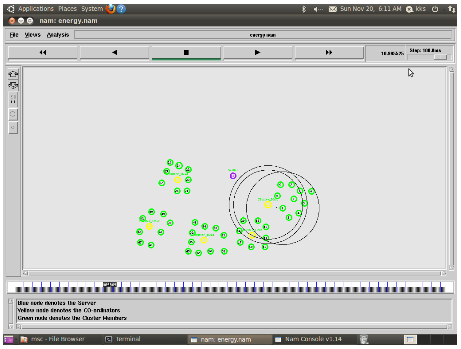
Energy Consumption =Total Energy - Remaining Energy

Energy Efficiency = Remaining Energy

Duration of the delay from beginning to end

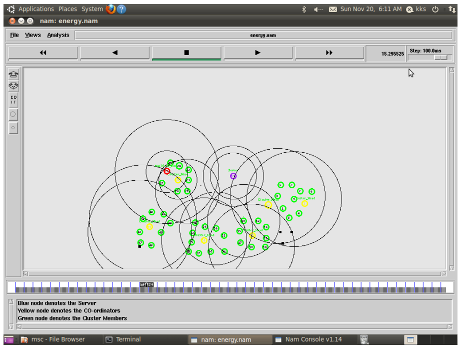
The length of time it takes for each packet to leave the sender node and travel to the destination is defined as delay.

Delay = Received Time – Transmitted Time / Number of Packets



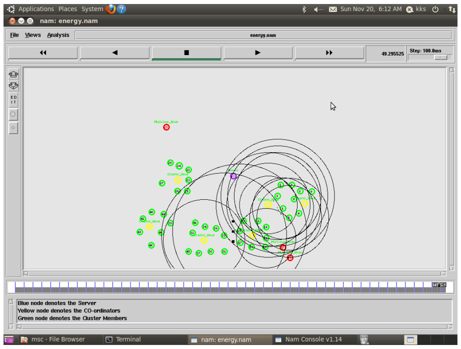
```
Blue node denotes the Server
Yellow node denotes the CO-ordinators
Green node denotes the Cluster Members
```

Fig. 4. Network communication between nodes



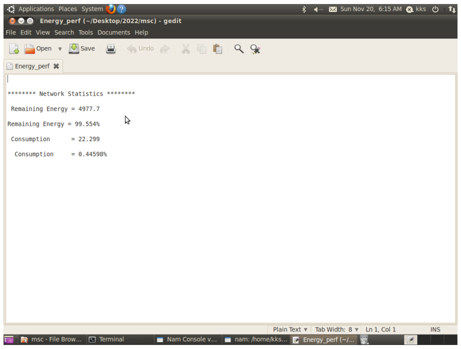
```
Blue node denotes the Server
Yellow node denotes the CO-ordinators
Green node denotes the Cluster Members
```

Fig. 5. Wormhole Detection



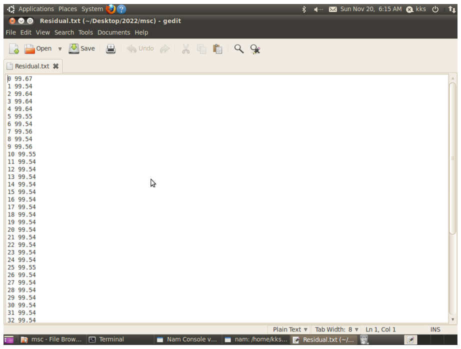
```
Blue node denotes the Server
Yellow node denotes the CO-ordinators
Green node denotes the Cluster Members
```

Fig. 6. Discover all Wormhole nodes



```
******** Network Statistics ********

 Remaining Energy = 4977.7

Remaining Energy = 99.554%

 Consumption      = 22.299

  Consumption     = 0.44598%
```

Fig. 7. Efficiency and Consumption Calculation



```
0 99.67
1 99.54
2 99.64
3 99.64
4 99.64
5 99.55
6 99.54
7 99.56
8 99.54
9 99.56
10 99.55
11 99.54
12 99.54
13 99.54
14 99.54
15 99.54
16 99.54
17 99.54
18 99.54
19 99.54
20 99.54
21 99.54
22 99.54
23 99.54
24 99.54
25 99.55
26 99.54
27 99.54
28 99.54
29 99.54
30 99.54
31 99.54
32 99.54
```

Fig. 8. Residual Energy of all Nodes

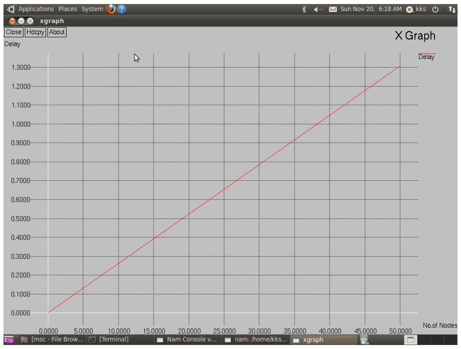
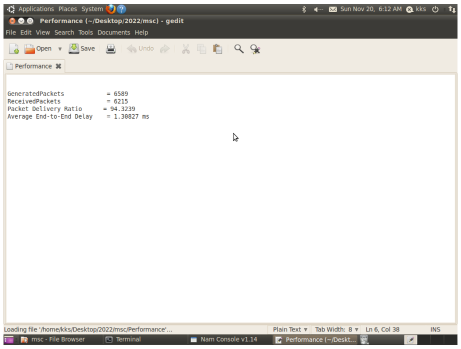


Fig. 9. Delay graph



```
GeneratedPackets           = 6589
ReceivedPackets            = 6215
Packet Delivery Ratio     = 94.3239
Average End-to-End Delay    = 1.30827 ms
```

Fig. 10. Performance Calculation(PDR and Delay)

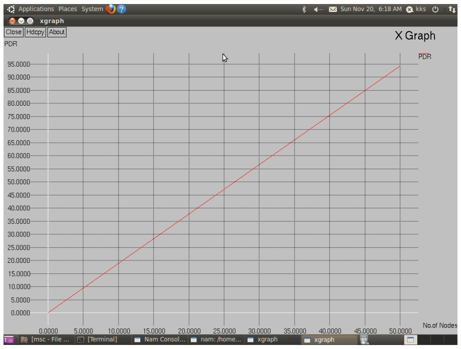


Fig. 11. PDR graph

Packet Delivery Ratio

The proportion of all packets created by the client node to all packets obtained by the end target.

PDR = Received Packets/Generated Packets * 100

When the comparison study considers both the EEHRCP and the AD-PSO in addition to the advised.method, and after results for all of the techniques taken into consideration were evaluated, it was found that the suggested technique (i-AOMDV) had a higher delivery rate for all network sizes.

VII. Conclusion and Future Work

A. Conclusion

The methodology is used here to detect wormhole attack on clustered networks. Sensor nodes and different routes are deployed in the early stages. AOMDV allows sending and receiving ways to be created. The LNCA technique, which organises the nodes into clusters, with the degree of similarity between the nodes being of paramount importance; is employed with regard to the study design, grouping the nodes during their initial deployment stage. Cluster formation is als otaken into consideration at this stage. The performance assessments of the suggested technique based on variables like point-to-point delay are shown in graphs in the analysis section. Packet dropped ratio and energy consumption.

B. Limitations of the Work

- Prevention is a big challenge in this work.
- Wormhole detection is only possible.
- We can't detect other attacks such as black-holes, vampire

C. Future Work

Integrate detection and prevention mechanisms to find malicious nodes and deliver more packets. Using the neighboring node's address as the bait's target address instigates RREP to bait the malicious node and respond, thereby tracking down the malicious node and preventing the attack. Use the Network Simulation Tool (NS2) to perform experimental simulations under various network conditions and evaluate performance metrics concerning packet delivery rate, delay, overhead, throughput, and energy.

References

[1] Alluhaidan, A. 2013. "Recommender System Using Collaborative Filtering Algorithm." School of Computing and Information Systems 10 (4): 155.

[2] Pathak, S., Jain, S. (2016). "A novel weight-based clustering algorithm for routing in MANET." Wireless Networks, 22(8), 2695–2704.

[3] Pathak, S., Dutta, N., Jain, S. (2014)." An improved cluster maintenance scheme for mobile AdHoc networks." In IEEE 2014 international conference on advances in computing, communications, and informatics (pp. 2117–2121).

[4] Pathak, S., Jain, S. (2017). "An optimized stable clustering algorithm for mobile ad hoc networks." EURASIP Journal on Wireless Communications and Networking, 2017(1), 1–11.

[5] Pathak, S., Jain, S. (2016). "A novel weight-based clustering algorithm for routing in MANET." Wireless Networks-The Journal of Mobile Communication, Computation, and Information, 21(8), 1–10.

[6] Munir, A., Gordon-Ross, A., Ranka, S. (2013). "Multi-core embedded wireless sensor networks: Architecture and applications." IEEE Transactions on Parallel and Distributed Systems, 25(6), 1553–1562.

[7] Kuorilehto, M., Hannikainen, M., Hamalainen, T. D. (2005)." A survey of application distribution in wireless sensor networks." EURASIP Journal on Wireless Communications and Networking, 2005 (5), 859712.

[8] Singh, S., Saini, H. S. (2021)." Learning-based security technique for selective forwarding attack in clustered WSN." Wireless Personal Communications, 118(1), 789–814.

[9] Sundararaj, V., Selvi, M. (2021). "Opposition grasshopper optimizer based multimedia data distribution using user evaluation strategy". Multimedia Tools and Applications. https:// doi. org/ 10. 1007/ s11042-021- 11123-4.

[10] Abbasi, A. A., Younis, M. (2007)." A survey on clustering algorithms for wireless sensor networks." Computer communications, 30, 2826–2841.

[11] Yu, Y., Krishnamachari, B., Prasanna, V. K. Issues in designing middleware for wireless networks. Department of EE Systems, University of Southern California.

[12] Mahalik, N. P. (2007). "Sensor networks and configuration: Fundamentals, standards, platforms, and applications."

[13] Luo, J., Hubaux J. -P. (2005). "Joint mobility and routing for lifetime elongation in wireless sensor networks." IEEE INFOCOM.

[14] Ughade, S., Kapoor, R. K., Pandey, A. (2014). "An overview on wormhole attack in wireless sensor network: Challenges, impacts, and detection approach". International Journal of Recent Development in Engineering and Technology. Intelligent Ad-Hoc-On Demand Multipath Distance Vector

[15] Gowthul Alam, M. M., Baulkani, S. (2017). "Reformulated query-based document retrieval using optimised kernel fuzzy clustering algorithm". International Journal of Business Intelligence and Data

[16] Mining, 12(3), 299. 15. Sundararaj, V. (2016)." An efficient threshold prediction scheme for wavelet-based ECG signal noise reduction using variable step size firefly algorithm." The International Journal of Intelligent Systems, 9(3), 117–126.

[17] Gowthul Alam, M. M., Baulkani, S. (2019). "Geometric structure information based multi-objective function to increase fuzzy clustering performance with artificial and real-life data." Soft Computing, 23(4), 1079–1098.

[18] Sundararaj, V. (2019)." Optimized denoising scheme via opposition-based self-adaptive learning PSO algorithm for wavelet-based ECG signal noise reduction. "International Journal of Biomedical Engineering and Technology, 31(4), 325.

[19] Gowthul Alam, M. M., Baulkani, S. (2019). "Local and global characteristics-based kernel hybridization to increase optimal support vector machine performance for stock market prediction". Knowledge and Information Systems, 60(2), 971–1000

[20] Sundararaj, V., Muthukumar, S., Kumar, R. S. (2018)." An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks." Computers Security, 77, 277–288.

[21] Vinu, S. (2019). "Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm." Wireless Personal Communications, 104(1), 173–197.

[22] Sharma, N., Singh, U. (2014)." Various approaches to detect Wormhole attack in wireless sensor networks". A Monthly Journal of Computer Science and Technology, IJCSMC, 3(2), 29–33.