Secure Routing using ISMO for Wireless Sensor Networks

M.Supriya[1], Dr.T.Adilakshmi[2]

[1]Associate Professor & HOD, Dept of Information Technology, Swami Vivekananda Institute of Technology, JNTUH, Secunderabad, Telangana, India
[2] Professor&HOD, Dept of CSE, Vasavi College of Engineering, Osmania University, Hyderabad, Telangana, India

Received Date: 13 November 2021
Revised Date: 16 December 2021
Accepted Date: 27 December 2021

Abstract — *The Wireless Sensor Network (WSN) is a type of wireless ad hoc network that uses densely packed small sensor nodes to monitor environmental changes. WSN is made up of battery powered, low cost sensor nodes with limited communication and computing capabilities. The security and restricted energy of the sensors, on the other hand, are identified as key challenges that affect the WSN's performance. As a result, secure cluster-based routing must be developed in order to achieve secure data transmission while minimizing node energy consumption. The clustering and secure Cluster Head (CH) selection are achieved in this paper using the K-Means algorithm, and then secure network routing is done using the SMO, whose fitness function takes into account four different values: trust, residual,, energy, distance, and node degree. As a result, ISMO-WSN based secure cluster-based routing is used to avoid blackhole attacks during data transfer by reducing packet loss, Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), routing overhead, and the average energy consumption is used to evaluate the proposed ISMO-WSN.In addition, the ISMO-WSN is evaluated using an existing method called Secure Routing Protocol based on Multi objective Ant colony optimization (SRPMA). The ISMO-WSN approach has a Packet Loss Ratio (PLR) of 3.57 % for 10 blackhole nodes; the routing overhead of this ISMO method is 0.067J for 10 blackhole attacks. An average energy utilization of the ISMO-WSN method is 1.38 J for 10 blackhole nodes.*

Keywords - *K-means clustering, ISMO-WSN (Improved spider monkey optimization-Wireless Sensor Network), trust, Blackhole attacks, packet delivery ratio, packet Loss ratio, Spider Monkey Optimization(SMO), SRPMA.*

I. INTRODUCTION

WSN is made up of a large number of sensors that monitor different environmental conditions such as sound, humidity, temperature, and so on [1]. The sensor nodes broadcast the changes seen in the environment to the sink or Base Station (BS) [2]. The WSN is being employed in a variety of sectors, including agriculture, education, military, and medicine [3]. When a sensor node in a WSN sends and receives data packets, it typically dissipates its energy. Since the sensor node is driven by a non-rechargeable battery, it only lasts a few months/years [4]. With that, the nodes are grouped into clusters, and CH is chosen from each cluster. and CH is selected from each cluster for minimizing the energy consumption. Here, the nodes in the clusters are communicated by using their respective CH [8] [9] [10].

When the BS is within its communication range, the CH directly transmits the data to the BS in cluster-based routing. Otherwise, the CH sends data to the BS via multi-hop communication with intermediate CHs [7]. Furthermore, because it is deployed in unattended and hostile locations, this WSN is vulnerable to attacks [8]. In general, connection problems, node failures, and malicious nodes occur in the WSN, disrupting the data transmission's reliability and stability [9]. The trust values are then computed in order to provide the secure channel that is used to accomplish secure communication in the WSN [10]. The network is divided into several clusters in this research utilizing the secure path identified from the ISMO algorithm. This secure data transmission results in less packet loss over the network. The organization of this paper is given as follows: The recent works related to secure data transmission in the WSN are described in Section 2. The secure cluster-based routing using ISMO-WSN is clearly given in Section 3. The results and discussion of this ISMO-WSN method are shown in Section 4. Finally, the conclusion is made in Section 5.

II. RELATED WORKS

Pavani, M. and Rao, P.T [16] developed the Secure Cluster-Based Routing Protocol (SCBRP) to obtain secure data transmission. In this SCBRP, clustering and routing were accomplished by using the adaptive Particle Swarm Optimization (PSO) and improved firefly algorithm, respectively. Moreover, four inputs such as the number of rounds, key size, hash value, and block size were considered in the fuzzy logic approach to verifying the security level of the nodes. Here, the node with a lesser security level is mitigated from the network. However, this SCBRP was failed to analyze in the large-scale environment.

Selvi, M et al. [17] presented the Energy-Aware Trust-Based Secure Routing Algorithm (EATSRA) in that trust values were utilized to identify the malicious nodes. An optimal and secured path was obtained by using the decision tree-based routing method. Subsequently, the decision about the routing was effectively made by using the Spatio-temporal constraints.

Dhand, G. and Tyagi, S.S [18] developed the Secure Multi-tier Energy Efficient Routing (SMEER) method. Here, the clustering and section of CH were accomplished by using the hybrid algorithm of K-means and ant lion optimization. This SMEER protocol was enhanced the security and energy utilization by providing elliptic curve cryptography along with spherical grid multi-tier routing. The packet loss over the network was reduced by using the spherical grid-based routing during the transmission time. But, the SMEER was considered only the distance and elliptic curve in the fitness function. This work failed to analyze the routing overhead that occurred in the network.

Shankar et al. [19] presented Grouped Grey Wolf Search Optimization (GGWSO) based CH selection. This GGWSO method was considered four different values such as distance, delay, energy, and security during the CH selection. The level of security was calculated by using the fuzzy scale in the GGWSO. However, the selection process of CH was affected when the security demand and rank were not satisfied in the network.

Ziwen Sun et al. [20] developed the SRPMA for improving the security in WSN. The ant colony algorithm was used as a multi-objective routing by using the residual energy and the trust value. Moreover, the integration of confliction processing and D-S evidence theory was used to compute the trust degree of the node. Subsequently, the node with higher trust was considered in routing to minimize the packet loss over the network. The developed SRPMA was failed to include distance among the CHs and node degree of the nodes during the routing path generation.

III. ISMO-WSN METHOD

In this ISMO-WSN method, secure data transmission between the nodes is achieved by using the ISMO. Here, the ISMO considers four important fitness values such as trust, residual energy, distance, and node degree. These fitness functions are used to modify the SMO to avoid blackhole attacks during the data transmission. Moreover, this method is used to minimize the energy utilization of the nodes.

A. Clustering by K-Means algorithm

The K-means algorithm is used in this ISMO method for clustering the network into k clusters. This K-means algorithm is an unsupervised clustering that uses a Euclidian distance for clustering the network. Moreover, this K-means algorithm results in high intra-cluster similarity and less inter-cluster similarity. Equation (1) expresses the Euclidian distance used in the clustering process.

$$Dist = \sqrt{\left(x_i - x_j\right)^2 - \left(y_i - y_j\right)^2} \qquad (1)$$

Where, $x_i \& y_i$, and $x_j \& y_j$ Are the coordinates of the node i and j.

B. Overview of SMO

The social activities of Spider Monkeys (SMs) [16] were a major inspiration for SMO. This SMO is mainly based on the foraging activities of Spider Monkey (SM). This SMO has various phases that are explained as follows:

a) Local leader phase

At first, an initial population (M) of SMs is generated, as shown in equation (2). The current swarm is updated in this local leader phase, and a new trial location is generated for each SM to update the current swarm. Specifically, the trial location is updated based on the random number, location of the local leader, and current position. The perturbation rate value is used to define the probability of the solution getting updated in the SMO. Equation (3) shows the generation of trail position of the SMs.

$$SM_{ij} = SM_{minj} + Rand(0,1) \times \left(SM_{maxj} - SM_{minj}\right) \qquad (2)$$

$$SM_{new\,ij} = SM_{ij} + Rand(0,1) \times \left(LL_{kj} - SM_{ij}\right) + Rand(-1,1) \times \left(SM_{rj} - SM_{ij}\right) \qquad (3)$$

Where the location of SMi in a dimension of j is represented as SM_{ij}; location of local group leader k in a dimension of j is represented as LL_{kj} and a uniform random number among the 0 and 1 is represented as $Rand(0,1)$. This uniform random number is generated for each dimension. The location of the SM is updated when the generated location has an improved fitness value than the current location.

b) Global leader phase

Similar to the local leader stage, this phase also updates the location of the SMs. In this phase, only one dimension is randomly chosen, and it is updated over the SMO. Here, the probability value is used to define which SM is going to be updated between the entire population. The ith spider monkey's probability is calculated as shown in equation (4).

$$prob_i = 0.9 \times \left(\frac{Fitness_i}{Max\ Fitness}\right) + 0.1 \qquad (4)$$

The trial location update is expressed in equation (5).

$$SM_{new\,ij} = SM_{ij} + Rand(0,1) \times \left(GL_j - SM_{ij}\right) + Rand(-1,1) \times \left(SM_{rj} - SM_{ij}\right) \qquad (5)$$

Where the location of the global leader in a dimension of j is represented as GL_j. The comparison between the fitness of newly produced location and current location is frequently made to identify the better location.

c) Global and local leader learning phase

In this global learning stage, the SM with optimal fitness is updated as a global leader. Moreover, the greedy selection is utilized for updating the local leader. In that, the location of SM with the best fitness is considered as an updated location of the local leader.

d) Local leader decision phase

In the local leader decision stage, the location of the local leader isn't updated to the predefined threshold and is specified as LocalLeaderLimit. In this LocalLeaderLimit, the initialization of the population in an arbitral manner or the cooperative information between global and local leaders is used to update all the SM's of that respective small group. Equation (6) shows the location update accomplished in the local leader decision process.

$$SM_{new\ ij} = SM_{ij} + Rand(0,1) \times \left(GL_j - SM_{ij}\right) + Rand(0,1) \times \left(SM_{ij} - LL_{kj}\right)$$

$$SM_{new\ ij} = SM_{ij} + Rand(0,1) \times \left(GL_j - SM_{ij}\right) + Rand(0,1) \times \left(SM_{ij} - LL_{kj}\right) \qquad (6)$$

From equation (6), it is known that the spider monkey's updated dimension is attracted to the global leader and resists against the local leader.

e) Global leader decision phase

This stage is utilized to monitor the global leader's location, and the global leader separates the population into smaller groups when it is not updated up to the limit of the global leader. Here, the local leader learning is initiated for selecting the local leader in the generated groups. Moreover, the global leader merges the separated groups into a single group when there is a huge amount of groups are created, and the global leader location is not updated in the decision phase.

C. Secure CH selection using ISMO

A secure CH is selected in the network using the ISMO under the constraints of blackhole attacks. Four different fitness values are used to modify the SMO, including trust, residual energy, the distance between nodes, and node degree. Select an optimal and secure CH between the nodes. A clear description of the CH selection is given as follows:

a) Representation and Initialization for CH selection

The SM's dimension is equal to the number of CHs that must be picked in the network.. Consider, the i the spider monkey is $SM_i = (SM_i^1, SM_i^2, .., SM_i^r)$, where each position of $SM_i^r = (x_i^r, y_i^r)$ And $1 \leq r \leq D$ denotes the node's Identification (ID). The node ID is mapped to the node's two-dimensional coordinates in this case.

b) Fitness function formulation

There are four different fitness functions as trust, residual energy, the distance among the nodes, and node degree are considered during the CH selection. The description of the fitness values are explained as follows:

c) Trust value of the node

The trust value of each node is regarded as a key fitness metric in this approach to boost resilience against blackhole assaults. Mutual trust is used to achieve reliable communication between nodes at a set period of time. The trust value is determined by the packet transmission ratio between nodes I and j. The trust value is defined as the ratio of the number of transmitted packets to the number of collected data packets, as shown in equation (7).

$$Tr_{i,j}(t) = \frac{P_{i,j}^T(t)}{P_{i,j}^R(t)} \qquad (7)$$

Where Tr represents the trust; the number of transmitted and collected packets are represented as $P_{i,j}^T$ and $P_{i,j}^R$. As a result, the fitness function's trust value is used to mitigate blackhole attacks.

d) Residual energy

The CHs of the clusters collect the data packets from the normal nodes, and the collected data is transmitted to the BS. The CH consumes a lot of energy to carry out the aforementioned duties. As a result, during data transmission, the node with high energy is selected. Equation (8) shows the residual energy of the node.

$$RE = \frac{1}{E_i} \qquad (8)$$

Where, E_i Specifies the ith node residual energy.

d) Distance

This is a Euclidean distance calculated between one node to another node. The energy consumption is minimized by generating the data transmission path with a lesser distance to the BS.

f) Node degree

The amount of nodes connected to the respective node is defined as node degree. Here, the node with a less node degree is preferred for reliable communication.

$$Fitness = Tr + RE + Dist + ND \qquad (9)$$

In the ISMO, the fitness function generated in equation (9) is employed in equation (4) to complete the location update. The coordinates in the ISMO population are updated using local and global leader phases based on this fitness function. The secure CHs between the group of nodes is then provided by this ISMO location update. Following that, these secure CHs are utilized to establish a secure network connection.

D. Secure routing using ISMO

This ISMO can be used to select the secure routing path via CHs to the BS. Here, the secure path is selected based on four different fitness functions such as trust, residual energy, distance, and node degree.

a) Representation and initialization for secure route selection

In this phase, each SM denoted the data transmission path from the CH to the BS. Here, the SM's dimension is equal to the amount of CHs in the network. Consider, the i the spider monkey is $SM_i = (SM_i^1, SM_i^2, .., SM_i^r)$, where each position of $SM_i^r = (x_i^r, y_i^r)$ And $1 \leq r \leq D$ represents the next hop CH.

b) Route selection

For determining the routing path, the ISMO employs the same fitness function as in section 3.3.2. To construct the routing path, ISMO-based routing employs control messages similar to the ad hoc on-demand distance vector routing protocol. The ISMO uses three control messages: Route Request (RREQ), Route Reply (RREP), Route Error (RERR), and hello (HELLO). The RREQ message is transmitted throughout the network during the route discovery process. The RREP message is then transmitted to the next-hop node, which has a higher fitness function**.** Here, the RREP message is transmitted to the source CH through the reverse route for generating the routing path. Whenever the source CH gets the RREP message, the data transfer via the network is initiated. The fitness function is used to select an appropriate secure path from the source CH to the BS. Similarly, HELLO is used to keep the routes updated.

IV. RESULTS AND DISCUSSION

The results and discussion of the ISMO method are clearly described in this section. For this paper, the NS-2.34 simulator is used along with the Ubuntu 16.04 OS platform to evaluate this method's performance. In this ISMO method, K-means clustering, ISMO-based CH selection, and path generation are developed for obtaining secure data transmission over the network. To analyze the performance of the ISMO method, 100 nodes are randomly deployed in the area of $1200\,m \times 1200\,m$. Here, the network is analyzed with the blackhole attacks for analyzing the performances of the ISMO method.

A. Performance analysis

The ISMO method is evaluated by means of PDR, PLR, routing overhead, and average energy consumption. Moreover, the ISMO method is compared with the SRPMA [20] for evaluating the ISMO method. The performance analysis is given as follows:

a) PDR

PDR is the relation between the number of packets received at the BS and the number of packets delivered by the source node. Equation (10) is used to calculate the PDR.

$$PDR = \frac{\sum_{i=1}^{n} P_i^R}{\sum_{i=1}^{n} P_i^T} \times 100\% \qquad (10)$$

Where an amount of source code used to transmit the data packets is represented as n; P_i^R and P_i^T Represented the received and forwarded packets over the network.

Table 1. Performance analysis of PDR for ISMO with SRPMA

Number of blackhole attacks	SRPMA [20]	ISMO
2	93 %	96.17 %
4	90.8 %	97.70 %
6	89.5 %	97.95 %
8	88 %	96.17 %
10	85.5 %	96.42 %

Table 1 provides the performance comparison of the PDR with SRPMA [20]. For a better analysis of the PDR, the ISMO method is verified for varying blackhole attacks. Table 1 concluded that this method achieves higher PDR than the SRPMA [20]. In the ISMO method, the source node identifies the node with a higher trust value during the routing path transmission. This helps to improve the PDR of the ISMO under the constraints of blackhole attacks.

b) PLR

PLR is the relation between the number of packets dropped and the number of packets delivered by the source node, which is expressed in equation (11).

$$PLR = \frac{\sum_{i=1}^{n} P_i^T - \sum_{i=1}^{n} P_i^R}{\sum_{i=1}^{n} P_i^T} \times 100\%$$

(11)

Table 2. Performance analysis of PLR for ISMO withSRPMA

Number of blackhole attacks	SRPMA [20]	ISMO
2	7 %	3.82 %
4	9.2 %	2.29 %
6	10.5 %	2.04 %
8	12 %	3.82 %
10	14.5 %	3.57 %

The PLR comparison of the ISMO with SRPMA [20] Table 2. The ISMO method achieves less PLR when compared to the SRPMA [20]. The PLR of the ISMO method is 3.57 % for 10 blackhole nodes, which is less when compared to the SRPMA [20]. The mitigation of blackhole attacks during the routing is used to minimize the packet loss in the ISMO method. Moreover, node failure is avoided in this method by using the residual energy in the fitness function of the ISMO.

c) Routing overhead

The amount of control packets created in the network defines the routing overhead, and equation (12) shows an average routing overhead.

$$Routing\ overhead = \frac{1}{N}\sum_{i=1}^{n} CP_i$$

(12)

Where the number of experiments is represented as N and the control packet is represented as CP.

Table 3. Performance analysis of routing overhead for with SRPMA

Number of blackhole attacks	SRPMA [20]	ISMO
2	0.46	0.051
4	0.48	0.052
6	0.5	0.065
8	0.49	0.074
10	0.54	0.067

Table 3 provides the performance comparison of the routing overhead for ISMO with SRPMA [20]. Table 3 concluded that the ISMO method achieves lesser routing overhead than the SRPMA [20]. The routing overhead of the ISMO method is 0.067 for 10 blackhole attacks that are less when compared to the SRPMA [20]. The ISMO method forwards only lesser control packets while generating the path, so it results in lesser overhead in the network.

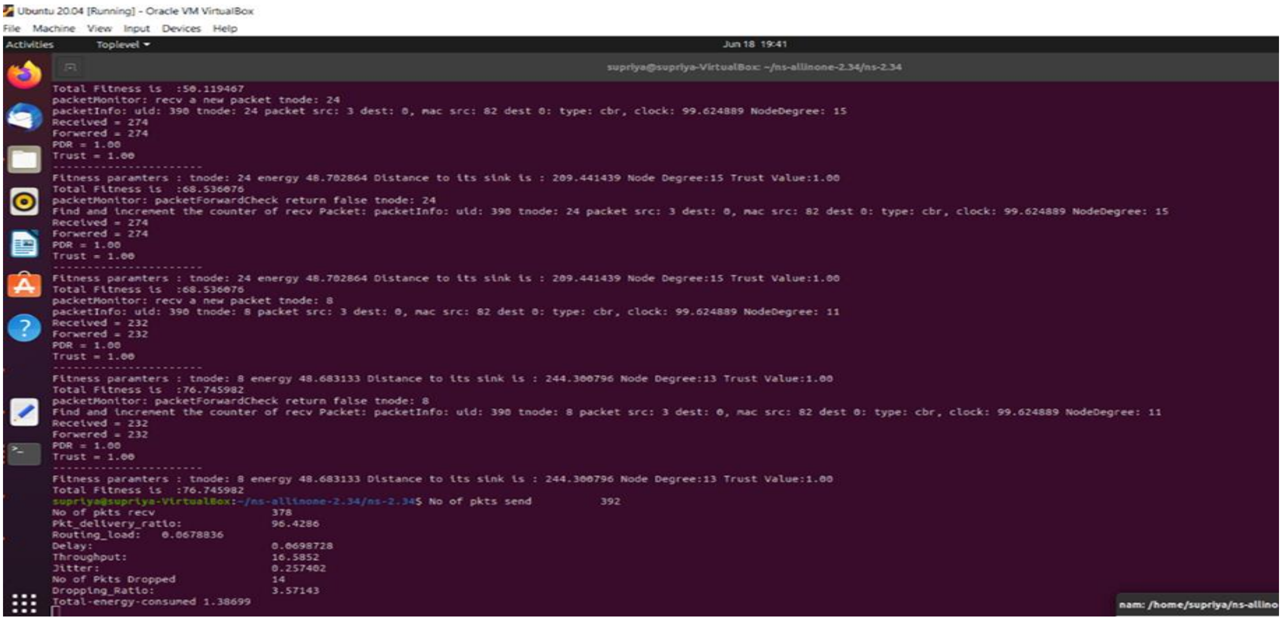
d) Average Energy Consumption

Average energy consumption is the amount of energy utilized by all the nodes of the WSN during the communication.

Table 4. Performance analysis of average energy consumption for with SRPMA

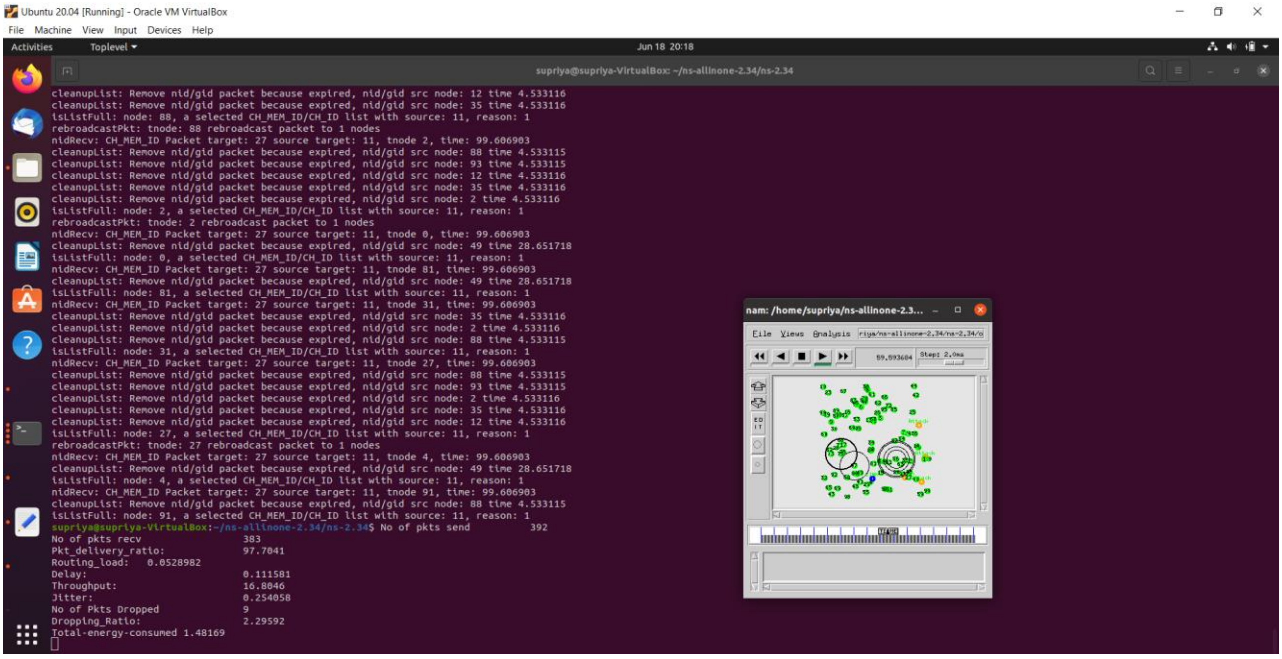
Number of blackhole attacks	SRPMA [20]	ISMO
2	39 J	1.36 J
4	37.5 J	1.48 J
6	36 J	1.42 J
8	35 J	1.39 J
10	33 J	1.38 J

An average energy consumption comparison of the ISMO method with SRPMA [20] is shown in Table 4. The ISMO method achieves less energy consumption than the SRPMA [20]. For example, the average energy utilization of the ISMO method is 1.38 J for 10 blackhole nodes, which is less when compared to the SRPMA [20]. Here, the energy consumption of the ISMO method is mainly reduced by identifying the shortest path during communication.


Ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Toplevel
Jun 18 19:41
supriya@supriya-VirtualBox: ~/ns-allinone-2.34/ns-2.34
nam: /home/supriya/ns-allino

```
Total Fitness is  :50.119467
packetMonitor: recv a new packet tnode: 24
packetInfo: uid: 390 tnode: 24 packet src: 3 dest: 0, mac src: 82 dest 0: type: cbr, clock: 99.624889 NodeDegree: 15
Received = 274
Forwered = 274
PDR = 1.00
Trust = 1.00
---------------------
Fitness paramters : tnode: 24 energy 48.702864 Distance to its sink is : 209.441439 Node Degree:15 Trust Value:1.00
Total Fitness is  :68.536076
packetMonitor: packetForwardCheck return false tnode: 24
Find and increment the counter of recv Packet: packetInfo: uid: 390 tnode: 24 packet src: 3 dest: 0, mac src: 82 dest 0: type: cbr, clock: 99.624889 NodeDegree: 15
Received = 274
Forwered = 274
PDR = 1.00
Trust = 1.00
---------------------
Fitness paramters : tnode: 24 energy 48.702864 Distance to its sink is : 209.441439 Node Degree:15 Trust Value:1.00
Total Fitness is  :68.536076
packetMonitor: recv a new packet tnode: 8
packetInfo: uid: 390 tnode: 8 packet src: 3 dest: 0, mac src: 82 dest 0: type: cbr, clock: 99.624889 NodeDegree: 11
Received = 232
Forwered = 232
PDR = 1.00
Trust = 1.00
---------------------
Fitness paramters : tnode: 8 energy 48.683133 Distance to its sink is : 244.300796 Node Degree:13 Trust Value:1.00
Total Fitness is  :76.745982
packetMonitor: packetForwardCheck return false tnode: 8
Find and increment the counter of recv Packet: packetInfo: uid: 390 tnode: 8 packet src: 3 dest: 0, mac src: 82 dest 0: type: cbr, clock: 99.624889 NodeDegree: 11
Received = 232
Forwered = 232
PDR = 1.00
Trust = 1.00
---------------------
Fitness paramters : tnode: 8 energy 48.683133 Distance to its sink is : 244.300796 Node Degree:13 Trust Value:1.00
Total Fitness is  :76.745982
supriya@supriya-VirtualBox:~/ns-allinone-2.34/ns-2.34$ No of pkts send          392
No of pkts recv                 378
Pkt_delivery_ratio:             96.4286
Routing_load:   0.0678836
Delay:                          0.0698728
Throughput:                     16.5852
Jitter:                         0.257402
No of Pkts Dropped              14
Dropping_Ratio:                 3.57143
Total-energy-consumed 1.38699
```

Fig1 : Number of blackhole attacks:10,Total energy consumed :1.38699,PDR:96.4%


Ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Toplevel
Jun 18 20:18
supriya@supriya-VirtualBox: ~/ns-allinone-2.34/ns-2.34
nam: /home/supriya/ns-allinone-2.3...
File Views Analysis
riya/ns-allinone-2.34/ns-2.34/o
59.593684
Step: 2.0ms
EDIT
attack
TIME

```
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 12 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 35 time 4.533116
isListFull: node: 88, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
rebroadcastPkt: tnode: 88 rebroadcast packet to 1 nodes
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 2, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 88 time 4.533115
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 93 time 4.533115
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 12 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 35 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 2 time 4.533116
isListFull: node: 2, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
rebroadcastPkt: tnode: 2 rebroadcast packet to 1 nodes
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 0, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 49 time 28.651718
isListFull: node: 0, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 81, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 49 time 28.651718
isListFull: node: 81, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 31, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 35 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 2 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 88 time 4.533115
isListFull: node: 31, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 27, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 88 time 4.533115
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 93 time 4.533115
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 2 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 35 time 4.533116
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 12 time 4.533116
isListFull: node: 27, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
rebroadcastPkt: tnode: 27 rebroadcast packet to 1 nodes
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 4, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 49 time 28.651718
isListFull: node: 4, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
nidRecv: CH_MEM_ID Packet target: 27 source target: 11, tnode 91, time: 99.606903
cleanupList: Remove nid/gid packet because expired, nid/gid src node: 88 time 4.533115
isListFull: node: 91, a selected CH_MEM_ID/CH_ID list with source: 11, reason: 1
supriya@supriya-VirtualBox:~/ns-allinone-2.34/ns-2.34$ No of pkts send          392
No of pkts recv                 383
Pkt_delivery_ratio:             97.7041
Routing_load:   0.0528982
Delay:                          0.111581
Throughput:                     16.8046
Jitter:                         0.254058
No of Pkts Dropped              9
Dropping_Ratio:                 2.29592
Total-energy-consumed 1.48169
```

Fig2 : Number of blackhole attacks:4,Total energy consumed :1.48169,PDR :97.7%

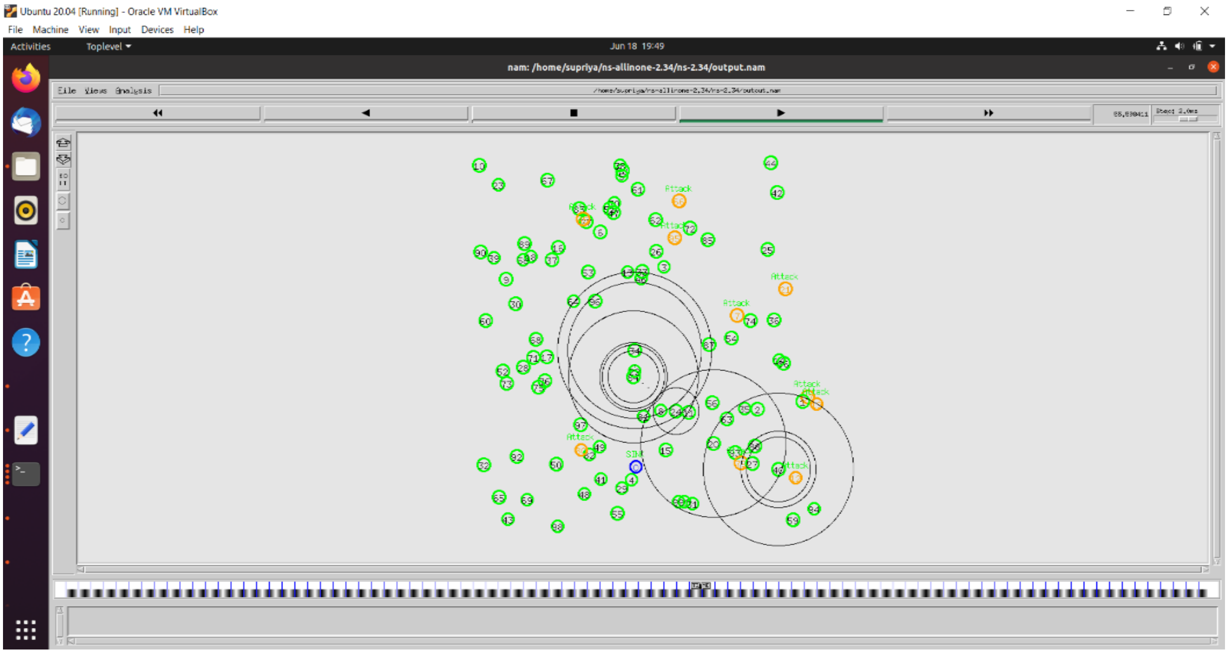

Ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Toplevel
Jun 18 19:49
nam: /home/supriya/ns-allinone-2.34/ns-2.34/output.nam
File Views Analysis
Attack
SINK

Fig 3: **Simulation results for 100 nodes using ISMO WSN for Packets transmission and packet drop**

V. CONCLUSION

Generally, the nodes in the WSN are susceptible to security threats, i.e., the blackhole attacks that exist in the network cause packet loss. Furthermore, the energy consumption of the nodes is also considered as the main issue due to the limited battery of the nodes. The ISMO-WSN method is suggested in this research for limiting the security vulnerabilities provided by blackhole attacks. Clustering with the K-means algorithm and safe CH selection using the ISMO method reduces the node's energy usage. The mitigation of blackhole attacks during the routing is used to minimize the packet loss in the ISMO-WSN method. Moreover, node failure is avoided by using the residual energy in the fitness function. The ISMO is also used to identify the secure transmission path via CHs to the BS. Trust, residual energy, distance, and node degree are four different fitness functions. The shortest path identification using ISMO minimizes the energy utilization of the nodes. As a result, the approach performs better than the SRPMA method. The approach has a packet loss ratio of 3.57% for 10 blackhole attacks, which is lower than the SRPMA method.

REFERENCES

[1] Kavidha, V. and Ananthakumaran, S., Novel energy-efficient secure routing protocol for wireless sensor networks with mobile sink. Peer-to-Peer Networking and Applications, 12(4) (2019) 881-892.

[2] Vijayalakshmi, V. and Senthilkumar, A., USCDRP: an unequal secure cluster-based distributed routing protocol for wireless sensor networks. The Journal of Supercomputing, 76(2) (2020) 989-1004.

[3] AlFarraj, O., AlZubi, A. and Tolba, A., Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, (2018) 1-11.

[4] Selvakumar, K., Sairamesh, L. and Kannan, A., An intelligent energy-aware secured algorithm for routing in wireless sensor networks. Wireless Personal Communications, 96(3) (2017) 4781-4798.

[5] Azharuddin, M., Kuila, P. and Jana, P.K., Energy-efficient fault-tolerant clustering and routing algorithms for wireless sensor networks. Computers & Electrical Engineering, 41 (2015) 177-190.

[6] Rodrigues, P. and John, J., Joint trust: an approach for trust-aware routing in WSN. Wireless Networks, (2020) 1-16.

[7] Deepa, C. and Latha, B., HHSRP: a cluster-based hybrid hierarchical secure routing protocol for wireless sensor networks. Cluster Computing, 22(5) (2019) 10449-10465.

[8] Alghamdi, T.A., Secure and energy-efficient path optimization technique in wireless sensor networks using DH method. IEEE Access, 6 (2018) 53576-53582.

[9] Darabkh, K.A., Al-Maaitah, N.J., Jafar, I.F. and Ala'F, K., EA-CRP: a novel energy-aware clustering and routing protocol in wireless sensor networks. Computers & Electrical Engineering, 72 (2018) 702-718.

[10] Sureshkumar, C. and Sabena, S., Fuzzy-Based Secure Authentication and Clustering Algorithm for Improving the Energy Efficiency in Wireless Sensor Networks. Wireless Personal Communications, 112(3) (2020) 1517-1536.

[11] Logambigai, R., Ganapathy, S. and Kannan, A., Energy-efficient grid-based routing algorithm using intelligent fuzzy rules for wireless sensor networks. Computers & Electrical Engineering, 68 (2018) 62-75.

[12] Rahayu, T.M., Lee, S.G. and Lee, H.J., A secure routing protocol for wireless sensor networks considering secure data aggregation. Sensors, 15(7) (2015) 15127-15158.

[13] Ye, Z., Wen, T., Liu, Z., Song, X. and Fu, C., A security fault-tolerant routing for multi-layer non-uniform clustered WSNs. EURASIP Journal on Wireless Communications and Networking, 2016(1) (2016) 1-12.

[14] Sharma, R., Vashisht, V. and Singh, U., eeTMFO/GA: a secure and energy-efficient cluster head selection in wireless sensor networks. Telecommunication Systems, (2020) 1-16.

[15] Sahoo, R.R., Sardar, A.R., Singh, M., Ray, S. and Sarkar, S.K., A bio-inspired and trust-based approach for clustering in WSN. Natural Computing, 15(3) (2016) 423-434.

[16] Pavani, M. and Rao, P.T., Adaptive PSO with optimized firefly algorithms for secure -cluster-based routing in wireless sensor networks. IET Wireless Sensor Systems, 9(5) (2019) 274-283.

[17] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H.K. and Kannan, A., An energy-aware trust-based secure routing algorithm for effective communication in wireless

sensor networks. Wireless Personal Communications, 105(4) (2019) 1475-1490.

[18] Dhand, G. and Tyagi, S.S., SMEER: Secure multi-tier energy-efficient routing protocol for hierarchical wireless compared to the SRPMA 20 (2019).

[19] Shankar, A., Jaisankar, N., Khan, M.S., Patan, R. and Balamurugan, B., A hybrid model for security-aware cluster head selection in wireless sensor networks. IET Wireless Sensor Systems, 9(2) (2018) 68-76.

[20] Sun, Z., Wei, M., Zhang, Z. and Qu, G., Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. Applied Soft Computing, 77 (2019) 366-375.