A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network

D. Giji Kiruba¹, J. Benita² and D. Rajesh³

¹Research Scholar, Department of Electrical and Electronics Engineering, ¹²Assistant Professor, Department of Electrical and Electronics and Communication Engineering, ¹²Noorul Islam Centre for Higher Education, Kanyakumari, Tamil Nadu, India
³Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India

E-mail: d.jijikiruba@gmail.com, beni.bless@gmail.com, rajeshd936@gmail.com

(Received 8 October 2023; Revised 1 November 2023, Accepted 22 November 2023; Available online 27 November 2023)

Abstract - A collection of wireless nodes that may be installed at any location and at any time without requiring an established network structure is called a mobile wireless sensor network. The problem of network performance arises from the mobility of nodes and their misbehaviour. Network performance is negatively impacted by data loss and sensor node misbehaviour. In certain cases, there are malicious sensor nodes that are designed to destroy the network’s capacity. This work aims to identify hostile nodes using an irregular set technique. The route entry table’s broadcasting metadata helps identify rogue nodes. Every sensor node in the network broadcasts information about adjacent nodes and maintains a sentry table. Premeditated data delivery proportion, throughput, delay, packet drop, and fault rate are used to estimate broadcasting record parameters. In the NS2 environment, mobile nodes with varying velocities are simulated. To generate an information table, mobile nodes with varying speeds are examined based on their broadcasting records. On the basis of guidelines taken from the irregular set tactic table, good and bad nodes are distinguished. Packets are disseminated along the shortest path that doesn’t contain any malicious nodes. The results of the proposed technique show that an irregular set tactic increases throughput, network capability, data delivery percentage, and end-to-end delay reduction in mobile sensors.

Keywords: Information Classification, Malicious Node, Irregular Set, Route Entry Table

I. INTRODUCTION

The Mobile Wireless Sensor Network (MWSN), which is made up of thousands of mobile sensors placed in a network, allows them to connect with multiple other mobile sensors. The primary objective of routing protocol design in MWSNs, which have limited resources, is to minimise energy consumption and prolong the lifespan of mobile systems. Clusters are the smaller subsystems that make up the entire system. Mobile sensor networks are used in home computerization, atmosphere observation, flood and fire detection, and other applications. Each cluster has its own cluster head (CH). Sensor nodes transmit recorded events to the base station via CH broadcast. Extending the time is a crucial data collection strategy associated with the suggested clustered routing methods. In WSN, mobility is a crucial problem that modifies topology and causes packet losses or delays in the target node [1-4]. Hierarchical routing and other energy-efficient routing strategies pose a serious challenge to reducing the amount of energy needed to broadcast packets and gather data. Measuring mobility variables is necessary to improve clustering techniques [8-9]. Aggregated data transmitted either single-hop or multi-hop to the base station from clustered nodes. Higher exceptional energy is found in CH than in clustered nodes.

Malevolent entities infiltrate the network as a result of energy loss, path disruption, and sensor nodes dozing off. Malevolent nodes in a network constantly reveal dangerous dangers that undermine the system’s overall functionality. Secure and reliable routing strategies, authentication techniques, and cryptography are used to ensure secure data transmission. In addition to inside attacks, defence is a difficult task similar to passive attacks [10]. Malevolent nodes from outside the system also attempt to get in. Unusual set tactics used by both stationary and mobile sensor nodes can be used to identify anomalous behaviour among sensor nodes.

Research work is organized as sections II illustrate the review of literature. Irregular set tactic based malicious node recognition by information classification in section III. Simulation Outcome and Investigation are demonstrated in section IV. Finally, section V concluded research work and future work are designed.

II. REVIEW OF LITERATURE

A creative hierarchical clustering technique for WSN is called LEACH-(Low-Energy Adaptive-Clustering Hierarchy) [11], [12]. Events from sensor nodes are broadcast to base station (BS) with the assistance of a nearby CH [13], [14]. The sensor nodes’ mobility is not maintained during each cycle after the setup stage. Owing to irregular grouping in LEACH packet loss acquisitions [15]. Using the Simulated Annealing technique, the base station analyses k-optimal groups and resolves CHs (CHs) related...
to the sensor node’s remaining energy level, position, and remoteness in LEACH-C (Low-Energy Adaptive-Clustering Hierarchy-C) [16], a centralised adaptation of the LEACH methodology. The K-Means technique [17-20] divides a set of nodes into clusters based on a distinguishing feature associated with intra- and inter-cluster communication. Centroid and k-(CHs) CHs for each cluster iteration.

In MANETs, malicious sensor nodes are identified and separated. Intrusion Detection Systems (IDS) and Optimised Link State Routing (OLSR) in MANET expand security strategies to detect malicious sensor nodes in the network. End-to-end (E2E) communication between the source and target sensor nodes is a strategy used in OLSR. To isolate hostile sensor nodes from neighbouring sensor nodes and the network, malevolent sensor nodes were removed from the routing table. The sender can select a different verified path to reach the target sensor node by eliminating the malicious sensor node [21].

A general framework for classifying mobile nodes activity depends on MANET. Under some conditions, mobile nodes within a network might become self-centered or malicious, completely destroying the network’s capability. In a network, good and bad mobile nodes are grouped using a rough set methodology. Rough sets eliminate unrelated mobile nodes from networks and produce straightforward policies [22].

In MANET, the detection of packet-plummeting mobile nodes uses the DSR technique to identify malicious nodes by observing neighbouring mobile nodes within the network. Because the MANET has limited energy, all of the mobile nodes should not be able to see every other node in the network. The eavesdropping method is causing the mobile node’s aliveness to decline. The CH observing node is the centre of the entire clustered mobile. When necessary, broadcast this message to the source mobile node and other cluster supervising mobile nodes. CH supervising mobile nodes locate and pinpoint packet-plummeting mobile nodes in their clustered region and maintain assurance to every mobile node in their clustered region. The entire network is divided into tiny virtual clusters by this approach, and a supervising mobile node is chosen for each cluster to detect packet droppers. Overhead and false recognition in networks can decrease [23].

IDS are used in [24] and [25] to study attentive measurements generated by various mobile nodes at various instances. Used to observe current conditions and estimate future computations pertaining to the location and origin of problems. Interrupter avoidance and recognition are defined for securing wireless environments [26]. Nodes process entire events and distinguish between them, taking appropriate action when they detect unusual activity from an intruder. Organisations that are knowledge-based solve problems by keeping specifics related to a problem condition in their knowledge base for the purpose of investigating and eliminating intruders [27]. A knowledge base is a collection of composite organisations that hold data and measurements for later use in computations and problem solving. An approach to building a knowledge base and implementing an appraisal scheme for system security [28]. In clustered related techniques, centralised settings offer greater control over routing and congestion inside the system. Clusters are created when nodes are put together, and each cluster is overseen by a node acting as the CH [29]. CHs communicate with the base station regarding events and pathways from nodes that have a direct or multi-hop structure. Nodes in clusters make events and activities, which are overseen by CHs [30]. In order to obtain the duration of nodes and the continuation of all processes for a lengthy period of time and comparison with the suggested approach, CHs are chosen [31].

III. PROPOSED WORK

There are three different types of mobile energy intensity sensor nodes.

1. Regular mobile nodes;
2. Intermediate mobile nodes; and
3. Superior mobile nodes.

Based on their behaviour, mobile nodes are categorised as better, average or worse using irregular set tactics for these three kinds of sensor nodes.

A. Working Process

The suggested strategy is put into practice as follows.

1. The suggested network strategy comprises of a BS with a heterogeneous system and a variety of sensor nodes. In MWSNs, broadcasting factors are comparable to routing methods. Mobile nodes’ energy intensities are determined.
2. The total energy level of the mobile nodes is computed; if this energy level is zero, both the node and the system are dead. If the network cannot function, it will enter a setup and stable state.
3. Information categorization using an irregular set approach to identify malicious mobile nodes.

B. Set-up State

In the Set-up State, CH is calculated. Equation 9–10 represents the proportion of REMeas/OPENeas that represents the constraints as remaining and opening energy. The comparable method of calculating the remoteness constraint is to take the ratio of the average remoteness of all nodes from the base station, or Remote(i)/ARremote, to the remoteness of each individual node. TNS is represented by the total number of adjacent sensor nodes.

i. Assessed as a possibility for all sensor nodes together. Due to varying energy levels, regular mobile nodes, intermediate mobile nodes, and superior mobile nodes will have different probabilities. We estimate the threshold for each group of sensor nodes.
ii. An arbitrary number \( A_n \) is formed in correspondence. In the network, \( A_n \) value is assessed for each sensor node individually and contrasted with a threshold. A node assumes \( A_n < \text{evaluated responsibility for CH} \) if an evaluated threshold is met; otherwise, it is a cluster member node.

1. Selecting CH

A mathematical model is used to evaluate the CH choice. Node remoteness from BS is measured by \( R_{remote}(i) \). \( AR_{remote} \) is the mean distance between all sensor nodes within a base station. Choosing CH is based on mathematically.

\[
R_{remote}(i) = \sqrt{(R_{remote}(x)(i)-BS_x)^2+(R_{remote}(y)(i)-BS_y)^2} \quad (1)
\]

\[
AR_{remote} = \frac{1}{n} \sum (R_{remote}(x)(i)-R_{remote}(x)(j))^2 + (R_{remote}(y)(i)-R_{remote}(y)(j))^2 \quad (2)
\]

When, \( R_{Enode}(i) > IE_0 \),

\[
P_{norm} = \frac{P}{1+f\alpha+f0\beta} \quad (3)
\]

\[
P_{inter} = \frac{P(1+\beta)}{(1+f\alpha+f0\beta)} \quad (4)
\]

\[
P_{advance} = \frac{P(1+\alpha)}{(1+f\alpha+f0\beta)} \quad (5)
\]

Where, \( R_{Enode}(i) \) is remaining energy of node \( i \)

\( IE_0 \) - Initial energy

\( f, f_0\) - fraction of superior nodes and

\( \alpha, \beta\) - extra energy factor among superior and intermediary mobile nodes

If \( R_{Enode}(i) \leq IE_0 \),

\[
P_{norm} = k \times \frac{P}{1+f\alpha+f0\beta} \quad (6)
\]

\[
P_{inter} = k \times \frac{P(1+\beta)}{(1+f\alpha+f0\beta)} \quad (7)
\]

\[
P_{advance} = k \times \frac{P(1+\alpha)}{(1+f\alpha+f0\beta)} \quad (8)
\]

The potential for regular, intermediate, and superior mobile nodes is assessed using equations (3–8). Equations (9–11) are used to determine thresholds for regular, intermediate, and superior mobile nodes. A system’s thresholds are compared to any number of complete nodes. If a given node’s random number falls below the threshold, it is chosen as the CH superior node; nodes that cross the threshold after it are chosen as intermediary nodes; the rest nodes are chosen as ordinary mobile nodes.

C. Steady Condition State

In this mode, data broadcasting is carried out while data relaying protocols are taken into account.

i. Once the CH has been chosen, calculate the average distance between all of the nodes in the BS. Relaying data will be done in many or single hops, depending on average remoteness.

ii. Remoteness between CH and BS is then assessed. When the average distance is high, CH either directly relays data to BS or to another CH that is close by.

1. Malicious Node Identification

Relay rate averages are calculated in order to classify nodes connected to the resolution system. The unique characteristics of each mobile node whether benign or malevolent are used to classify nodes. The irregular set technique and dissimilar simulation are measured for divergent velocity in order to classify malicious moveable nodes in the system. Malicious mobile nodes are identified and removed from the network’s route entry table. For routing data, update the route entry table. The technique that follows identifies malicious mobile nodes within the system.

a. Recognition of Malicious Mobile Node Algorithm

Begin

1. Simulation system with six mobile nodes.

2. Relaying metrics of mobiles nodes are evaluated

Data deliverance proportion

\[ PDP = \frac{\text{Total packets arrived}}{\text{Total packets lost}} \]

E2Edelay

\[ E2E-delay = \frac{\text{Receiving time} - \text{Forwarded time}}{\text{Entire amount of Connections}} \]

Throughput

\[ TP = \frac{\text{Obtained packet size}}{\text{(initial time-End time)}} \]

Error percentage of mobile node

\[ EP = \frac{\text{Arrived Packets}}{\text{Originated Packets}} \]

3. To evaluate relaying metrics of mobile node simulation is analyzed with diverse velocity for entire mobile nodes.

4. Develop resolution policy related to relaying metrics.

5. Categorize mobile nodes based on policy either good or malicious.

6. Construct route entry table from relaying metrics and apply irregular set tactic to recognize mobile malicious node.

7. Confiscate malicious node from route entry table and revise route entry table.

8. Achieve routing procedure.

end
2. Relaying Metrics of Mobile Node

In order to avoid the needless route invention process, the route entry table gathers complete routes from the source to the target mobile node. Due to flooding, which causes a significant delay before relaying the initial packet, the route innovation technique in on-demand routing methods is extremely expensive in terms of time, energy, and bandwidth use of the network. The successful completion of the route entry table is a prerequisite for the performance of the approaches. When data is relayed over an unsuitable path, more traffic is generated, and routing delays are warranted in order to identify broken links. One tactic to lessen the effects of an unsatisfactory path (TTL) is to remove route entries after a brief Time-to-Live. If the TTL is too long, small, appropriate routes are rejected, and new route discovery may cause severe routing delays and traffic. To avoid unnecessary route innovation for frequently used routes, paths are aggregated in the route entry table.

Mobile nodes with sensors comprise the construct simulation network. metrics for mobile nodes that are determined by how well portable nodes function. Using broadcasting data, the performance of mobile nodes was evaluated.

Data Deliverance Proportion: The percentage between the number of packets actually received at the target nodes and the number of packets transmitted from the application layer is known as the data delivery proportion.

E2E Delay: E2E measures the system's mobile nodes' average efficiency. Both the target and source nodes are filled.

Throughput: Metric measuring the rapid delivery of data during the entire simulation. By splitting off whole packets that are approved by the full simulation process, it is premeditated.

Plummet Packets: Undelivered packages transmitted from mobile sources to a target mobile node.

Fault Rate: Data packet generated, divided by packet received in the destination node.

Duration: Sensor mobile node relaying metrics are planned at different speeds, e.g., 5, 10, 15, 20, and 25 ms. Five different nodes that were evaluated are listed in Tables I through VI.

**TABLE I RELAYING RECORD FOR MOBILE NODE0 WITH DIVERSE VELOCITY**

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>99.89</td>
<td>12.521</td>
<td>762.19</td>
<td>0</td>
<td>1</td>
<td>1157</td>
</tr>
<tr>
<td>10</td>
<td>99.546</td>
<td>14.032</td>
<td>753.33</td>
<td>11</td>
<td>0.9791</td>
<td>1141</td>
</tr>
<tr>
<td>15</td>
<td>98.32</td>
<td>17.920</td>
<td>772.58</td>
<td>8</td>
<td>0.9821</td>
<td>1162</td>
</tr>
<tr>
<td>20</td>
<td>99.10</td>
<td>21.232</td>
<td>741.84</td>
<td>13</td>
<td>0.9689</td>
<td>1137</td>
</tr>
<tr>
<td>25</td>
<td>98.15</td>
<td>18.417</td>
<td>752.52</td>
<td>15</td>
<td>0.9772</td>
<td>1142</td>
</tr>
</tbody>
</table>

**TABLE II RELAYING RECORD FOR MOBILE NODE1 WITH DIVERSE VELOCITY**

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>99.8736</td>
<td>20.572</td>
<td>746.81</td>
<td>11</td>
<td>0.989</td>
<td>1158</td>
</tr>
<tr>
<td>10</td>
<td>98.9951</td>
<td>16.656</td>
<td>748.95</td>
<td>17</td>
<td>0.984</td>
<td>1154</td>
</tr>
<tr>
<td>15</td>
<td>97.2134</td>
<td>23.953</td>
<td>743.91</td>
<td>18</td>
<td>0.978</td>
<td>1147</td>
</tr>
<tr>
<td>20</td>
<td>97.0132</td>
<td>23.018</td>
<td>741.72</td>
<td>23</td>
<td>0.968</td>
<td>1135</td>
</tr>
<tr>
<td>25</td>
<td>99.8736</td>
<td>20.572</td>
<td>746.81</td>
<td>11</td>
<td>0.989</td>
<td>1158</td>
</tr>
</tbody>
</table>

**TABLE III RELAYING RECORD FOR MOBILE NODE2 WITH DIVERSE VELOCITY**

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>87.814</td>
<td>41.528</td>
<td>761.18</td>
<td>17</td>
<td>0.823</td>
<td>1167</td>
</tr>
<tr>
<td>10</td>
<td>88.791</td>
<td>37.917</td>
<td>778.61</td>
<td>16</td>
<td>0.734</td>
<td>1145</td>
</tr>
<tr>
<td>15</td>
<td>89.521</td>
<td>35.551</td>
<td>787.75</td>
<td>20</td>
<td>0.943</td>
<td>1172</td>
</tr>
<tr>
<td>20</td>
<td>90.167</td>
<td>33.714</td>
<td>775.18</td>
<td>15</td>
<td>0.861</td>
<td>1147</td>
</tr>
<tr>
<td>25</td>
<td>89.738</td>
<td>34.926</td>
<td>767.36</td>
<td>19</td>
<td>0.383</td>
<td>1162</td>
</tr>
</tbody>
</table>
TABLE IV RELAYING RECORD FOR MOBILE NODE3 WITH DIVERSE VELOCITY

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>86.3106</td>
<td>42.152</td>
<td>771.95</td>
<td>19</td>
<td>0.716</td>
<td>1127</td>
</tr>
<tr>
<td>10</td>
<td>83.1381</td>
<td>62.791</td>
<td>737.84</td>
<td>17</td>
<td>0.826</td>
<td>1181</td>
</tr>
<tr>
<td>15</td>
<td>81.6836</td>
<td>61.193</td>
<td>757.74</td>
<td>25</td>
<td>0.982</td>
<td>1139</td>
</tr>
<tr>
<td>20</td>
<td>79.8366</td>
<td>37.706</td>
<td>752.81</td>
<td>34</td>
<td>0.696</td>
<td>1161</td>
</tr>
<tr>
<td>25</td>
<td>80.9251</td>
<td>78.714</td>
<td>753.94</td>
<td>19</td>
<td>0.281</td>
<td>1122</td>
</tr>
</tbody>
</table>

TABLE V RELAYING RECORD FOR MOBILE NODE4 WITH DIVERSE VELOCITY

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>79.185</td>
<td>45.781</td>
<td>781.94</td>
<td>40</td>
<td>0.891</td>
<td>1159</td>
</tr>
<tr>
<td>10</td>
<td>68.390</td>
<td>57.956</td>
<td>724.87</td>
<td>48</td>
<td>0.893</td>
<td>1156</td>
</tr>
<tr>
<td>15</td>
<td>54.281</td>
<td>51.928</td>
<td>719.20</td>
<td>51</td>
<td>0.261</td>
<td>1187</td>
</tr>
<tr>
<td>20</td>
<td>80.170</td>
<td>78.180</td>
<td>775.61</td>
<td>57</td>
<td>0.103</td>
<td>1134</td>
</tr>
<tr>
<td>25</td>
<td>67.464</td>
<td>59.570</td>
<td>747.83</td>
<td>61</td>
<td>0.110</td>
<td>1145</td>
</tr>
</tbody>
</table>

TABLE VI RELAYING RECORD FOR MOBILE CH WITH DIVERSE VELOCITY

<table>
<thead>
<tr>
<th>Velocity ms</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>97.811</td>
<td>11.938</td>
<td>764.91</td>
<td>5</td>
<td>0.891</td>
<td>1157</td>
</tr>
<tr>
<td>10</td>
<td>99.935</td>
<td>19.521</td>
<td>787.27</td>
<td>7</td>
<td>0.983</td>
<td>1189</td>
</tr>
<tr>
<td>15</td>
<td>89.650</td>
<td>17.759</td>
<td>762.38</td>
<td>4</td>
<td>0.926</td>
<td>1178</td>
</tr>
<tr>
<td>20</td>
<td>95.201</td>
<td>22.947</td>
<td>749.81</td>
<td>11</td>
<td>0.894</td>
<td>1156</td>
</tr>
<tr>
<td>25</td>
<td>97.871</td>
<td>26.710</td>
<td>769.82</td>
<td>19</td>
<td>0.974</td>
<td>1169</td>
</tr>
</tbody>
</table>

D. Information Classification of Irregular Set Tactic

1. Irregular Set Tactic

Pawlak proposed the irregular set technique in 1982 as an arithmetic tool that compacts with imprecision and improbability. The imperceptibility relation defines the relationship between process and conceptualization. Every event, object, or entity in an irregular set tactic is described in a row, and every trait taken into consideration for an element characterised in a column is characterised in a column. This information table is prepared for the purpose of classifying the information. The entire universe is applied to a chosen trait in order to increase the original rules’ efficacy. Every attribute in the information classification elements has a same value and is imperceptible. Associate sets of the universe as conception have similar values of resolution qualities. A component of the universe’s conception is optimistic. The minimal union elementary set in a conception is a higher estimation of the conception, which is not a component of the lower estimation, while the maximum union elementary set in a conception is a lesser estimation. It arranges and provides useful information that is concealed by the IF-THEN resolution principle, including constructive information on the accountability of exacting qualities and their associated sets. If the boundary region has been used, the set is irregular; if it is vacant, the set is crispy.

2. Information Classification

Data classification is analysed using table rows to represent objects and columns to represent symbols. The information is classified as couple C=(U,T), where T is a finite trait of an occupied set for t: U→E where t∈T, set E_t is evaluation set, and U is a finite object of a nonempty set in the universe. Enclosing resolution features and information classifications in resolution structures improves information categorization. S= (U,T,U{s}), where s∉T, is the information categorization of the resolution structure. Situation attributes are elements and resolution qualities in T. Typically, qualities in resolution have two or more probabilities. The resolution categorization explains nearly all of the information related to representation. Similar or unnoticeable objects in the information table indicate multiple instances, and other features that are redundant are indicated in equation (1).

\[
SR(M) = \{(Y,Y')\in U^2|\forall y\in Mq(y) = q(y')\}
\]

Where SR(M) - similarity relation
M - imperceptibility relation
Irregular set tactic examination performed utilizing inferior and superior estimations shown below,

Inferior estimation
\[ M^*Y = \{ Y \in U : M(Y) \subseteq Y \} \quad (2) \]

Superior estimation
\[ M^*Y = \{ Y \in U : M(Y) \cap Y \neq \emptyset \} \quad (3) \]

Where \( M \subseteq T \) and \( Y \subseteq U \).

Estimation \( Y \) by building inferior and superior estimations, which are assessed in equations (2) and (3), using information restricted in \( M \). The full rough irregular set, technique set connects with two crispy estimates inferior and superior, but the granularity of information is indistinguishable from the accessible information. Whole elements that belong to a set are contained in inferior estimation sets. The border area and irregular set tactic that contain occupied set border area are the differences between inferior and superior estimations. Equation (4) shows how the irregular set technique differentiates quantitatively.

\[ \alpha_M(Y) = \frac{|M^*Y|}{|M^*Y|} \quad (4) \]

Where \( |Y| \) signify cardinality \( Y = \emptyset \).

If \( \alpha_M(Y) = 1 \), then set \( Y \) is crispy reverence to \( M \).
If \( \alpha_M(Y) < 1 \), then set \( Y \) is irregular reverence to \( M \).

Certain restricted trait sets are associated with least reductions, protecting universe portioning. Equation (5) allows for the evaluation of these reductions using the imperceptibility matrix.

\[ X_{xy} = \{ a \in A | a(k_i) \neq a(k_j) \} \text{ for } x,y=1 \ldots n \]
\[ a^*1 \ldots a^*m = \Lambda \{ V C^*_{xy} | 1 \leq y \leq n, X_{xy} \neq \emptyset \} \quad (5) \]

where \( X_{ij} = \{ a \in A \subseteq X_{ij} \} \). Determine the consequence of estimated reduction and result on information set after eliminating meticulous trait by equation (6)

\[ \alpha(L,M)=1-\gamma(L-\{ \alpha \},M/\gamma(L,M)) \quad (6) \]

Table VII indicates the classification of information. where characteristics of an event, object, or entity are listed in rows, and characteristics of an element are listed in columns.

**TABLE VII RELAYING RECORDS WITH DIVERSE VELOCITY OF AVERAGE COST OF MOBILE NODES**

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummets Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>99.7837</td>
<td>19.79</td>
<td>761.782</td>
<td>8</td>
<td>0.582</td>
<td>1178</td>
</tr>
<tr>
<td>1</td>
<td>97.8167</td>
<td>30.71</td>
<td>773.642</td>
<td>12</td>
<td>0.728</td>
<td>1127</td>
</tr>
<tr>
<td>2</td>
<td>89.3469</td>
<td>20.89</td>
<td>761.710</td>
<td>9</td>
<td>0.630</td>
<td>1156</td>
</tr>
<tr>
<td>3</td>
<td>84.8376</td>
<td>30.93</td>
<td>768.647</td>
<td>20</td>
<td>0.691</td>
<td>1167</td>
</tr>
<tr>
<td>4</td>
<td>87.8754</td>
<td>54.78</td>
<td>749.189</td>
<td>40</td>
<td>0.982</td>
<td>1118</td>
</tr>
<tr>
<td>5</td>
<td>78.8157</td>
<td>38.29</td>
<td>763.621</td>
<td>21</td>
<td>0.857</td>
<td>1171</td>
</tr>
</tbody>
</table>

Create an IF-THEN resolution policy using the shared values of all nodes involved in relaying records executed at different speeds.

- If Data deliverance proportion \( \geq 95 \) then resolution = big
- Else if data deliverance proportion \( \geq 81 \) then resolution = average
- Else if data deliverance proportion \( \leq 80 \) then resolution = inferior
- If E2E delay \( \leq 45 \) then resolution = inferior
- Else if E2E delay \( > 50 \) then resolution = big
- If Throughput \( > 760 \) then resolution = big
- Else if throughput \( < 755 \) then resolution = inferior
- If plummet packets \( < 10 \) then resolution = inferior
- Else if plummet packet \( < 20 \) then resolution = average
- Else if plummet packet \( > 25 \) then resolution = big
- If fault rate \( \geq 0.955 \) then resolution = inferior
- Else if fault rate \( \leq 0.956 \) then resolution = average
- Else if fault rate \( < 0.590 \) then resolution = big
- If duration \( \geq 1175 \) then resolution = big
- Else if duration \( \leq 1175 \) then resolution = average
- Else if duration \( \leq 1130 \) then resolution = inferior

**TABLE VIII CATEGORIZATION OF DIVERSE SENSOR MOBILE NODES**

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Data Deliverance Proportion</th>
<th>E2E Delay</th>
<th>Throughput</th>
<th>Plummet Packets</th>
<th>Fault Rate</th>
<th>Duration</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>B</td>
<td>I</td>
<td>B</td>
<td>I</td>
<td>I</td>
<td>B</td>
<td>Fine</td>
</tr>
<tr>
<td>1</td>
<td>B</td>
<td>I</td>
<td>B</td>
<td>I</td>
<td>A</td>
<td>I</td>
<td>Fine</td>
</tr>
<tr>
<td>2</td>
<td>A</td>
<td>I</td>
<td>B</td>
<td>I</td>
<td>A</td>
<td>A</td>
<td>Fine</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
<td>I</td>
<td>B</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Fine</td>
</tr>
<tr>
<td>4</td>
<td>A</td>
<td>B</td>
<td>I</td>
<td>B</td>
<td>B</td>
<td>I</td>
<td>Malicious</td>
</tr>
<tr>
<td>5</td>
<td>L</td>
<td>I</td>
<td>B</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Fine</td>
</tr>
</tbody>
</table>
The classification of various sensor mobile nodes is shown in Table VIII, where B stands for large, A for average, and I for inferior. The aforementioned policies classify node behaviours as harmful or benign. Resolution is fine if the following conditions are met: data deliverance proportion = big/average, E2E delay = inferior, throughput = big, plummeted packets = inferior/average, fault rate = inferior/average, and duration = big/average. Otherwise, malicious resolution results if the following conditions are met: data deliverance proportion = inferior, E2E delay = large, throughput = inferior, plummeted packets = large, fault rate = large, duration = inferior.

E. Examination of Data utilizing ISES

The resolution policy is obtained via the ISES (Irregular Set Examination System), which then applies the policy to identify malicious sensor mobile nodes within the network. ISES uses techniques and procedures in irregular sets to assess table information. The suggested method for identifying and putting into practise mobile malicious nodes was as follows.

Process:
1. Attach data to ISES.
2. Assess Reduce.
3. Create a resolution strategy.

IV. SIMULATION OUTCOME AND INVESTIGATION

There were no simulations in NS2. Six sensor mobile nodes are distributed uniformly across the simulated environment, forming a mobile atmospheric network covering an area of 1000 by 1000 metres throughout a 1200 second simulation period. In this study report, the CBR constant bit rate is used for testing. With a minimum velocity of 5 m/s and a maximum velocity of 25 m/s, the mobility representations generated by the Bon Motion tool are displayed in Table IX simulation atmosphere as,

<table>
<thead>
<tr>
<th>Factors</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>1200 sec</td>
</tr>
<tr>
<td>Total Mobile Nodes</td>
<td>6</td>
</tr>
<tr>
<td>Simulation region</td>
<td>1000 X 1000</td>
</tr>
<tr>
<td>Datarange</td>
<td>256 Bytes</td>
</tr>
<tr>
<td>Relaying Rate</td>
<td>10 packets/sec</td>
</tr>
</tbody>
</table>

Figure 3 shows a comparison between the packet delivery of the CORP methodology and the proposed tactic. The quantity of packets forwarded to BS for the irregular set strategies routing protocol is greater than that of CORP. The current method is illustrated in red, and the proposed approach is shown in green. It is evident that the packet delivery proportion of the suggested method outperforms that of the existing CORP.
The plummet packets ratios of the CORP methodology and the suggested way are contrasted in Figure 4. The number of Plummets packets for the irregular set strategy routing protocol is less than that of CORP. This is because the position of the remote sensor node is contained in the irregular set tactic. Plummets packets are the result of unsuccessful information delivery via a broadcast channel. This is how much data is lost as a result of the target sensor’s inability to receive data. The CORP approach is shown in red, while the suggested technique is shown in green. It makes sense that the packet loss of the suggested method is less than that of the current one.
The E2E latency of the suggested strategy and the CORP methodology are contrasted in Figure 5. E2E is decreased while employing an irregular set strategy routing approach as opposed to CORP. This is because routing information is incorporated into the irregular set technique. Consequently, the data was provided promptly. The recommended approach is shown by the green line, and the current methodology is shown by the red line. It makes sense that the suggested method requires less time than the CORP method.

Figure 6 shows a comparison between the CORP technique’s proficient energy and the suggested methodology’s proficient energy. The energy efficiency of sensor nodes is calculated in order to minimise reclustering. The irregular set technique has a higher energy level in mobile sensor nodes and CHs. The suggested system is shown by the green line, and the current system is shown by the red line. The higher energy level of the suggested technique compared to the CORP system makes sense.

Figure 7 Increase of Security level in mobile nodes
Figure 7 shows a comparison between the security levels of the CORP methodology and the proposed methods. The irregular set tactic method enhances security in BSs, CHs, and mobile sensor nodes as comparison to CORP. This is because the irregular set approach enhances network security by utilising mobility-based intrusion detection in BS, CHs, and mobile sensor nodes. The CORP energy efficient reliable routing algorithm offers less information security and only evaluates energy efficiency. A proposed project is shown by the green line, and an existing scheme is indicated by the red line. It makes sense that the security level of the proposed method is higher than CORP.

V. CONCLUSION AND FUTURE WORK

Because of the mobility environment and resource constraints, security in MSWN is a challenging assignment for academics. The system’s route entry database identifies malicious sensor mobile nodes connected to relaying records. Every mobile node in the network maintains a record of its neighbouring mobile nodes’ relaying information and route entry table. Relaying record sensors are used to classify mobile nodes based on irregular set theory, which determines if the nodes are malevolent or not. By preserving the division between the universe and the producer solution policy, irregular set strategies help eliminate superfluous traits and generate the lowest traits set as reduction, to develop the initial solution policy for classifying mobile sensor nodes. When a rogue mobile node is included in the generated route, data transmitters use different, shorter routes for relaying. Therefore, effectively separating the network’s falling mobile nodes from the event. Using the route entry table in the system, linkage breakdowns are quickly recognised. This methodology’s low reward is a fake recognition rate and decreased system transparency. The results of the simulation show that the current approaches are inferior to the data deliverance proportion, throughput, security, residual energy, and E2E latency. Future implementations will be able to identify fraudulent sensor mobile nodes in a network using neural networks, cross models, and fuzzy sets.

REFERENCES

A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network


