Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P), Vol.13, No.2, 2023, pp.53-63

DOI: https://doi.org/10.51983/ijiss-2023.13.2.3793

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

D. Giji Kiruba[1], J. Benita[2] and D. Rajesh[3]
[1]Research Scholar, Department of Electrical and Electronics Engineering,
[2]Assistant Professor, Department of Electronics and Communication Engineering,
[1&2]Noorul Islam Centre for Higher Education, Kanyakumari, Tamil Nadu, India
[3]Professor, 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 i nodes into n 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 $REM_{eng}/Open_{eng}$ 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 $R_{remote}(i)/AR_{remote}$, 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<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.

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

$$AR_{remote} = (1/n)* sqrt((R_{remote(x)}(i)- R_{remote(x)}(j))^2 + (R_{remote(y)}(i)-R_{remote(y)}(j))^2) \quad (2)$$

When,
$RE_{node}(i)>IE_0$,

$$P_{norm}=P/(1+f\alpha+f_0\beta) \quad (3)$$

$$P_{inter}=(P(1+\beta))/((1+f\alpha+f_0\beta) \quad (4)$$

$$P_{adavnce}=(P(1+\alpha))/((1+f\alpha+f_0\beta) \quad (5)$$

Where,
$RE_{node}(i)$ is remaining energy of node i
IE_0- Initial energy
f, f_0- fraction of superior nodes and
α,β-extra energy factor among superior and intermediary mobile nodes

If $RE_{node}(i)\leq IE_0$,

$$P_{norm}=k*(P/(1+f\alpha+f_0\beta)) \quad (6)$$

$$P_{inter}= k* ((P(1+\beta))/((1+f\alpha+f_0\beta)) \quad (7)$$

$$P_{adavnce}= k* ((P(1+\alpha))/((1+f\alpha+f_0\beta)) \quad (8)$$

$$T_{norm}= P_{norm}/ (1-P_{norm}(cmod(1/P_{norm})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_sdiv(1/P_{norm})*(1- REM_{eng}*Open_{eng}*NM \quad (9)$$

$$T_{inter}= P_{inter}/ (1-P_{inter}(cmod(1/P_{inter})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_sdiv(1/P_{inter})*(1- REM_{eng}*Open_{eng}*NM \quad (10)$$

$$T_{advance}= P_{inter}/ (1-P_{advance}(cmod(1/P_{advance})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_sdiv(1/P_{advance})* (1- REM_{eng}*Open_{eng}*NM \quad (11)$$

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
Data deliverance proportion
PDP = Total packets arrived/Total packets lost
E2Edelay
E2E-delay = (Receiving time−Forwarded time)/ Entire amount of Connections
Throughput
TP = Obtained packet size /(initial time-End time)
Error percentage of mobile node
EP = Arrived Packets/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. Constructroute 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 systems 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

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

TABLE II RELAYING RECORD FOR MOBILE NODE1 WITH DIVERSE VELOCITY

Velocity ms	Data Deliverance Proportion	E2E Delay	Throughput	Plummet Packets	Fault Rate	Duration
5	99.8736	20.572	746.81	11	0.989	1158
10	98.9951	16.656	748.95	17	0.984	1154
15	97.2134	23.953	743.91	18	0.978	1147
20	97.0132	23.018	741.72	23	0.968	1135
25	99. 8736	20.572	746.81	11	0.989	1158

TABLE III RELAYING RECORD FOR MOBILE NODE2 WITH DIVERSE VELOCITY

Velocity ms	Data Deliverance Proportion	E2E Delay	Throughput	Plummet Packets	Fault Rate	Duration
5	87.814	41.528	761.18	17	0.823	1167
10	88.791	37.917	778.61	16	0.734	1145
15	89.521	35.551	787.75	20	0.943	1172
20	90.167	33.714	775.18	15	0.861	1147
25	89.738	34.926	767.36	19	0.383	1162

TABLE IV RELAYING RECORD FOR MOBILE NODE3WITH DIVERSE VELOCITY

Velocity ms	Data Deliverance Proportion	E2E Delay	Throughput	Plummet Packets	Fault Rate	Duration
5	86.3106	42.152	771.95	19	0.716	1127
10	83.1381	62.791	737.84	17	0.826	1181
15	81.6836	61.193	757.74	25	0.982	1139
20	79.8366	37.705	752.81	34	0.696	1161
25	80.9251	78.714	753.94	19	0.281	1122

TABLE V RELAYING RECORD FOR MOBILE NODE4 WITH DIVERSE VELOCITY

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

TABLE VI RELAYING RECORD FOR MOBILE CH WITH DIVERSE VELOCITY

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

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: $U \rightarrow E_t$ where $t \in T$, 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 $s \notin T$, 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).

$$SR(M) = \{(Y,Y') \in U^2 | \forall_t \in M q(y) = q(y')\} \quad (1)$$

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

$$M^*Y = \{Y \in U : M(Y) \cap Y \neq \phi\} \quad (3)$$

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.

$$\alpha_M(Y) = |M*Y| / |M*Y| \quad (4)$$

Where |Y| signify cardinality $Y = \phi$.
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.

$$X_{xy} = \{a \in A |\ a(k_i) \neq a(k_j)\} \text{ for } x,y = 1 \ldots\ldots n$$
$$a^*_1 \ldots\ldots a^*_m = \Lambda \{V\ C^*_{xy} | 1 \leq y \leq x \leq n, X_{xy} \neq \emptyset \quad (5)$$

where $X^*ij = \{a^* | a \in Xij\}$. Determine the consequence of estimated reduction and result on information set after eliminating meticulous trait by equation (6)

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

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

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

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>= 95 then resolution = big
Else if data deliverance proportion >= 81 then resolution = average
Else if data deliverance proportion ≤80 then resolution = inferior
If E2E delay≤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 >= 0.955 then resolution = inferior
Else if fault rate ≤0.956&>= 0.590 then resolution = average
Else if fault rate ≤0.590 then resolution = big
If duration >=1175then resolution = big
Else if duration ≤1175&>= 1130 then resolution = average
Else if duration ≤1130 then resolution = inferior

TABLE VIII CATEGORIZATION OF DIVERSE SENSOR MOBILE NODES

Nodes	Data Deliverance Proportion	E2E Delay	Throughput	Plummet Packets	Fault Rate	Duration	Resolution
0	B	I	B	I	I	B	Fine
1	B	I	B	I	A	I	Fine
2	A	I	B	I	A	A	Fine
3	A	I	B	A	A	A	Fine
4	A	B	I	B	B	I	Malicious
5	L	I	B	A	A	A	Fine

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, plumet 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.
4. Use the classifier as Resolution trees to learn from the exercise data set.
5. A matrix of construct uncertainty.
6. Use the Utilize Response Policy to categories hostile mobile nodes.

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 IX SIMULATION FACTORS

Factors	
Time	1200 sec
Total Mobile Nodes	6
Simulation region	1000 X 1000
Datarange	256 Bytes
Relaying Rate	10 packets/sec

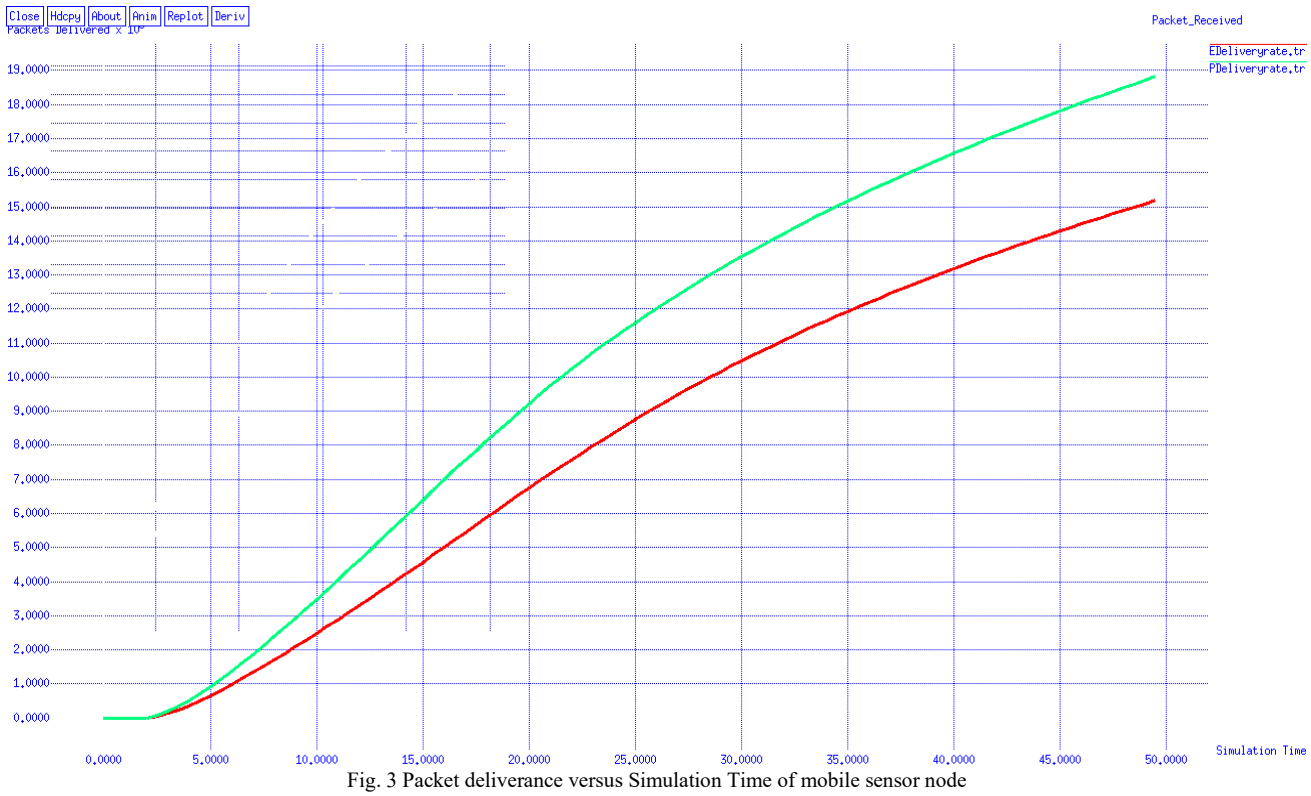

Fig. 3 Packet deliverance versus Simulation Time of mobile sensor node

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.

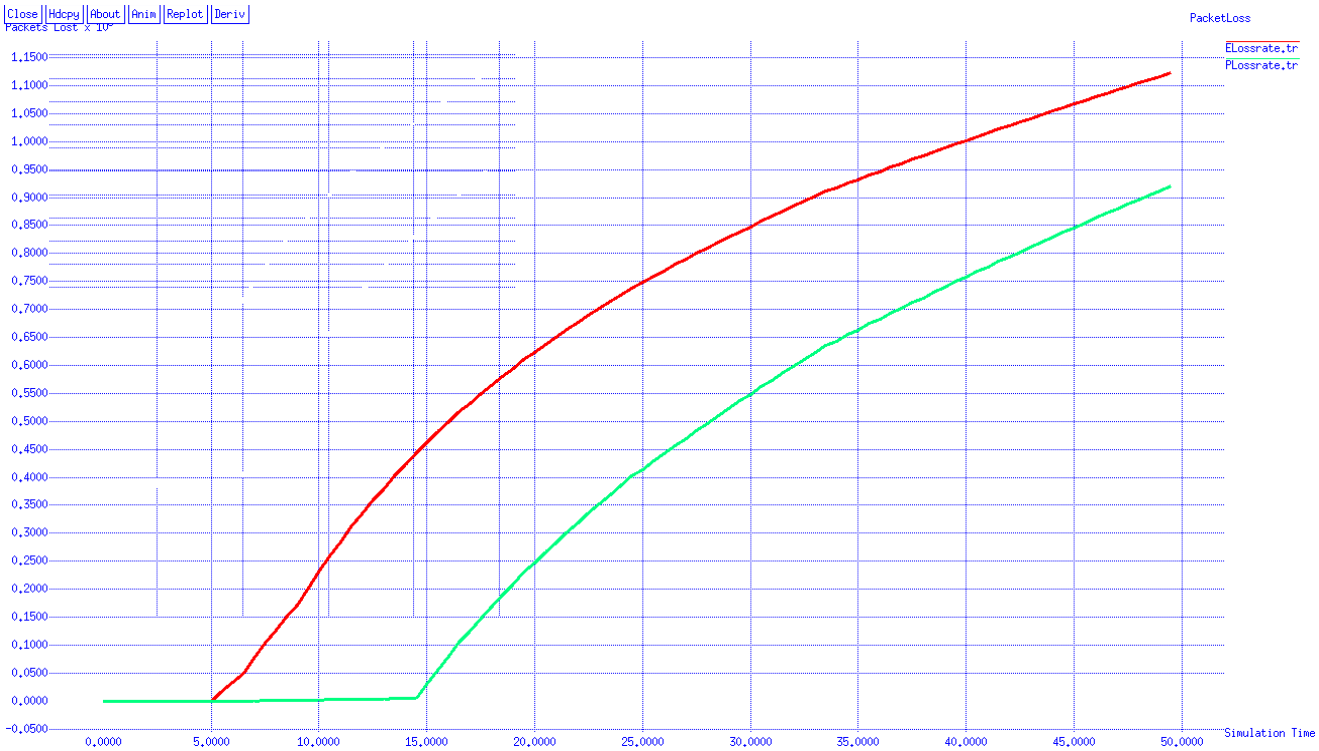

Fig. 4 Plummet packets versus Simulation Time of mobile sensor nodes

The plummet packets ratios of the CORP methodology and the suggested way are contrasted in Figure 4. The number of Plummet 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. Plummet 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.

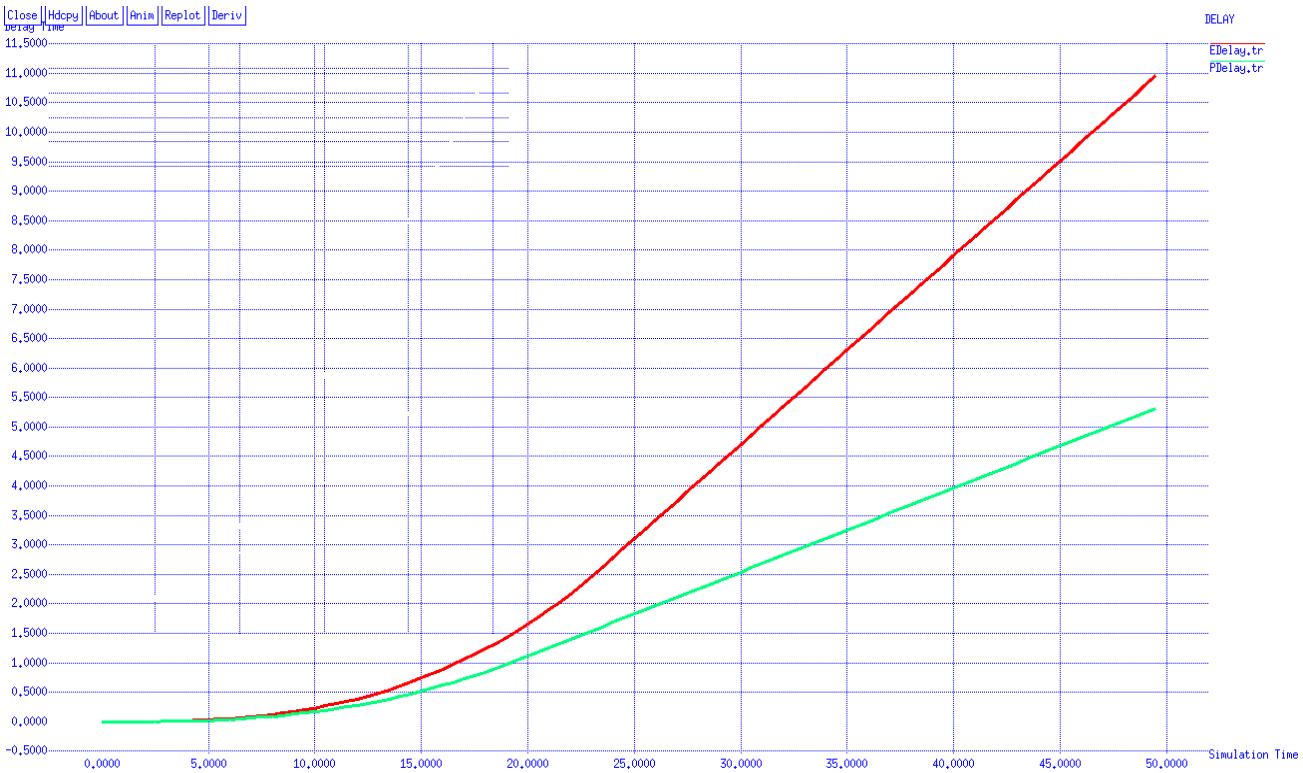

Fig. 5 E2E Delay in mobile sensor nodes

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.

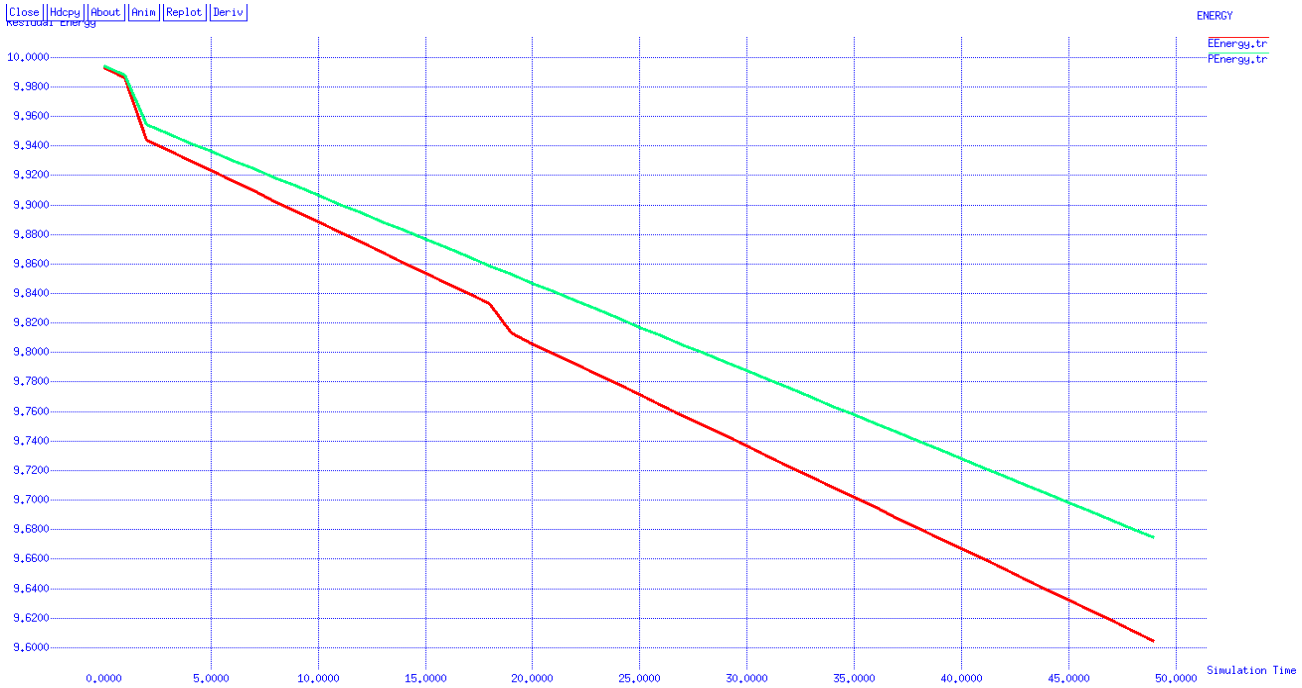

Fig. 6 Proficient Energy to Increase duration of Network

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.

Fig. 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

[1] Maya M. Warrier & Ajay Kumar. (2016). An Energy Efficient Approach for Routing in Wireless Sensor Networks. *Procedia Technology, 25,* 520-527.

[2] Amin Shahraki, Amir Taherkordi, Øystein Haugen & Frank Eliassen. (2020). Clustering objectives in wireless sensor networks: A survey and research direction analysis. *Computer Networks, 180*.

[3] Priyadarshi, R., Gupta, B. & Anurag, A. (2020). Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues. *The Journal of Supercomputing, 76*, 7333-7373.

[4] Rajesh, D., & Jaya, T. (2022). Energy competent cluster-based secured CH routing EC2SR protocol for mobile wireless sensor network. *Concurrency and Computation: Practice and Experience, 34*(1), e6525. DOI: 10.1002/cpe.6525.

[5] Gurjot Singh *et al.,* (2015). Classification of Wireless Sensor Networks Clustering Techniques. *International Journal of Applied Engineering Research, 10*(10), 24747-24757.

[6] Gholami, M. Taboun, M. S., & Brennan, R. W. (2019). An ad hoc distributed systems approach for industrial wireless sensor network management. *Journal of Industrial Information Integration, 15*, 239-246.

[7] Prabhu, Boselin. (2015). Distributed Clustering Using Enhanced Hierarchical Methodology for Dense WSN Fields. *International Journal of Applied Engineering Research, 10*(6).

[8] Serhani, A., Naja, N. & Jamali, A. (2020). AQ-Routing: mobility, stability-aware adaptive routing protocol for data routing in MANET-IoT systems. *Cluster Computing, 23*, 13-27.

[9] Alharbi, M. A., Kolberg, M. & Zeeshan, M. (2021). Towards improved clustering and routing protocol for wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking, 2021*(46).

[10] Wahid, A. & Kumar, P. (2015). A survey on attacks, challenges and security mechanisms in wireless sensor network. *International Journal for Innovative Research in Science and Technology, 1*(8), 189-196.

[11] Adnan Ismail Al-Sulaifanie, Subir Biswas, Bayez Khorsheed Al-Sulaifanie. (2017). AH-MAC: Adaptive Hierarchical MAC Protocol for Low-Rate Wireless Sensor Network Applications. *Journal of Sensors, 2017*, 1-15. DOI: https://doi.org/10.1155/2017/8105954.

[12] Santar Pal Singh & Sharma, S. C. (2015). A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks. *Procedia Computer Science, 45*, 687-695.

[13] Pundir, S., Wazid M., Bakshi A., & Singh D. P. (2021). Optimized Low-Energy Adaptive Clustering Hierarchy in Wireless Sensor Network. In: Deshpande P., Abraham A., Iyer B., Ma K. (eds) Next Generation Information Processing System. *Advances in Intelligent Systems and Computing, 1162*.

[14] Jasim, A. A., Idris, M. Y. I., Razalli Bin Azzuhri, S., Issa, N. R., Rahman, M. T., & Khyasudeen, M. F. (2021). Energy-Efficient Wireless Sensor Network with an Unequal Clustering Protocol Based on a Balanced Energy Method (EEUCB). *Sensors, 21*(3), 784.

[15] Muhammad K. Khan, Muhammad Shiraz, Qaisar Shaheen, Shariq Aziz Butt, Rizwan Akhtar, Muazzam A. Khan, & Wang Changda. (2021). Hierarchical Routing Protocols for Wireless Sensor Networks: Functional and Performance Analysis. *Journal of Sensors, 2021*.

[16] Alrashidi, M., Nasri, N., Khediri, S. *et al.,* (2020). Energy-Efficiency Clustering and Data Collection for Wireless Sensor Networks in Industry 4.0. *Journal of Ambient Intelligence and Humanized Computing.*

[17] Paulo Henrique Faria, João Felipe Coimbra Leite Costa & Marcel Antônio Arcari Bassani. (2021). Multivariate geostatistical simulation with PPMT: an application for uncertainty measurement. *Applied Earth Science.*

[18] Pal, R., Yadav, S., Karnwal, R. *et al.,* (2020). EEWC: energy-efficient weighted clustering method based on genetic algorithm for HWSNs. *Complex & Intelligent Systems, 6,* 391-400.

[19] Gantassi R., GouissemB.B., Othmen J. B. "Routing Protocol LEACH-K Using K-Means Algorithm in Wireless Sensor Network"., I: Barolli L., Amato F., Moscato F., Enokido T., Takizawa M. (2020). Web, Artificial Intelligence and Network Applications. WAINA 2020. *Advances in Intelligent Systems and Computing, 1150*.

[20] Cao, B., Deng, S., Qin, H. et al., (2021). A novel method of mobility-based clustering protocol in software defined sensor network. *EURASIP Journal on Wireless Communications and Networking, 2021,* 99.

[21] Dhananjayan, G. & Subbiah, J. (2016). T2AR: trust-aware ad-hoc routing protocol for MANET. *Springer Plus, 5,* 995.

[22] Mohit Jain, M. B. (2014). A Rough Set based Approach to Classify Node Behavior in Mobile Adhoc Networks. *Journal of Mathematics and Computer Science, 11*, 64-78.

[23] Anshu Chauhan, D. (2015). Detection of Packet Dropping Nodes in MANET using DSR Protocol. *International Journal of Computer Applications, 123*(7), 0975-8887.

[24] Mehmood, A. Khanan, A. Mohamed, A. H. H. M. & Song, H. (2018). ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET. *IEEE Access, 6,* 4452-4461.

[25] Zeeshan Ali Khan & Peter Herrmann. (2019). Recent Advancements in Intrusion Detection Systems for the Internet of Things. *Security and Communication Networks, 2019*.

[26] Hu, Z. Z., Leng, S., Lin, J. R. *et al.,* (2021). Knowledge Extraction and Discovery Based on BIM: A Critical Review and Future Directions. *Archives of Computational Methods in Engineering.*

[27] Umar, M. M. Mehmood, A. & Song, H. (2016). SeCRoP: Secure CH centered multi-hop routing protocol for mobile ad hoc networks. *Security and Communication Networks, 9*(16), 3378_3387.

[28] Balasubramanian Muthusenthil, Hyunsung Kim, & Surya Prasath, V. B. (2020). Location Verification Technique for Cluster Based Geographical Routing in MANET. *Informatica, 31*(1), 113-130.

[29] Zhang, W., Han, D., Li, K. C. *et al.,* (2020). Wireless sensor network intrusion detection system based on MK-ELM. *Soft Computing, 24*, 12361-12374.

[30] Rajesh, D., & Rajanna, G. S. (2022). CSCRT protocol with energy efficient secured CH clustering for smart dust network using quantum key distribution. *International Journal of Safety and Security Engineering, 12*(4), 441-448. DOI: https://doi.org/10.18280/ijsse.120404.

[31] Shanmugam, R., & Kaliaperumal, B. (2021). An energy-efficient clustering and cross-layer-based opportunistic routing protocol (CORP) for wireless sensor network. *International Journal of Communication Systems, 34*(14).