International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(1):50-61 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i01.0134

Energy Efficient Clustering Mechanism for Malicious Sensor Nodes in IOT Based MWSN

Giji Kiruba D[1]*, Benita J[1], Rajesh D[2]

[1]Department of Electrical and Electronics Engineering, Noorul Islam Centre for Higher Education, Kumaracoil-629 180, Tamil Nadu, India, [2]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. *Corresponding Author's Email: d.jijikiruba@gmail.com

Abstract

A mobile wireless sensor network (MWSN) is a collection of wireless nodes that may be set up anywhere and at any time without the need for a pre-existing network structure. Network performance is challenging factor due to nature of mobility and misbehaving nodes. Data loss and misbehaving in sensor nodes degrades performance of network. Some circumstances some malevolent sensor nodes predisposed to eradicate capability of network. The goal of this study is to use an irregular set approach to distinguish hostile nodes. Broadcasting information in route entry table identifies malicious node. Each sensor node in network preserves entry table and broadcast record regarding nearby nodes. To estimate broadcasting record metrics are premeditated as data deliverance proportion, throughput, delay, packet drop, fault rate. Mobile nodes with diverse velocity are simulated in NS2 environment which contains variable node clusters. Based broadcasting records of mobile nodes with diverse velocity are considered to create information table. Fine and malicious nodes are recognized based on rules derived in table of irregular set tactic. Shortest path without malicious node is elected to broadcast packets in the environment. Proposed tactic consequences reveal irregular set tactic amplifies network capability data deliverance percentage, throughput and dwindled end-to-end delay in mobile sensors.

Keywords: Information classification, Malicious Node, Irregular Set, Route entry Table, Internet of Things.

Introduction

Thousands of mobile sensors arranged in a network to form Mobile Wireless Sensor Network (MWSN) communicate with several other mobile sensors. In MWSN includes limited assets, so main designing goal of routing protocols to condense energy exploitation and enhance lifetime of mobile system. Entire system is spllited into sub-systems called clusters. Each cluster has its own cluster head (CH) Mobile sensor network utilized in residence computerization, atmosphere observation, flood recognition, fire recognition, etc.. CH broadcast captured events from sensor nodes to Base station. Enhancing duration is very significant data gathering tactics related with clustered routing approaches proposed. Mobility is a critical issue in WSN that changes topology loss packets or delay in target node (1-4). Energy resourceful routing tactics is hierarchical routing (5-7) are significant challenge to diminish energy utilization requisite to broadcast packets and congregate data information. Enhancing clustering methodologies mobility factors should be measured (8-9). Aggregated data from clustered nodes broadcast to base station either in single-hop or multi-hop. CH contains higher outstanding energy than clustered nodes.

Due to energy loss, path breakage and snoozing of sensor nodes malevolent enters into network. Malevolent nodes in network always exposed harmful threats which vitiate entire functionality of system. Authentication approaches, safe and sound routing tactics executes cryptography to guarantee secure communication of data. Protection beside inside attacks is complex process as passive attacks (10). Malevolent nodes from external also try to penetrate in system. Irregular behaviour among sensor nodes can recognize by irregular set tactic usage in CH and mobile sensor nodes. LEACH (Low-Energy Adaptive-Clustering Hierarchy) is inventive hierarchical clustering methodology for WSN (11-12). Sensor nodes events are broadcasted with help of nearby CH to base station (BS) (13-14). After setup stage does not sustain mobility of sensor nodes in every cycle. Due to inconsistent clustering in LEACH packet loss acquires (15)

(Received 16th October 2023; Accepted 05th January 2024; Published 30th January 2024)

LEACH-C (Low-Energy Adaptive-Clustering Hierarchy-C) (16) is a centralised adaptation of the LEACH methodology in which the base station evaluates k-optimal groups and resolves CHs associated with the remaining energy level of the sensor node, position, and remoteness using the Simulated Annealing tactic (SA). K-Means tactic (17-20) consists to separate set of i nodes into n clusters distinctive related with decisive factor of intra and inter cluster communication. Centroid for every cluster iteration and k-CHs.

Malevolent sensor nodes are recognition and segregation in MANETs. Optimized Link State Routing (OLSR) and Intrusion Detection Systems (IDS) in MANET enlarges security tactic to identify malevolent sensor nodes in network. OLSR tactic related with End-to-End (E2E) transmission among source and target sensor node. Malevolent sensor nodes eliminated from routing table to separate malevolent sensor nodes from nearby sensor nodes and network. Eradicating malevolent sensor node permits source to choose another authenticated path to target sensor node (21).

Rough set methodology to categorize mobile nodes activities in Mobile Ad hoc Network (MANET). In some circumstances mobile nodes in network turn into egocentric or malevolent node and obliterate capability of network. Good and terrible mobile nodes in network are categorized on rough set methodology. Rough set generates straightforward policy and eradicate unrelated mobile nodes from network (22).

Recognition of packet plummeting mobile nodes in MANET utilizes Dynamic Source Routing (DSR) approach to recognize malevolent mobile node observes nearby mobile nodes in network. Entire mobile nodes in MANET should not observe nearby node in network because it has constrained amount of energy. Aliveness of mobile node is degrading due to eavesdropping manner. Entire clustered mobile consist of observing node called CH. CH supervising mobile nodes determine and identify packet plummeting mobile nodes in clustered region and preserve assurance to entire mobile node in their clustered region and broadcast this message to source mobile node and other cluster supervising mobile node when necessary. This system partitions entire network to miniature virtual clusters and every cluster one supervising mobile node is elected to identify packet droppers. False recognition and overhead in network can diminish (23).

IDS utilized to investigate attentive measures produced by diverse mobile nodes at diverse instance (24, 25). Used for observing present circumstances and approximate upcoming calculations regarding position and derivation of trouble. Securing wireless environment interruption recognition and interruption avoidance are established (26). Entire events processed by nodes are distinguished and suitable measures are performed when recognition of irregular activity by an interloper. Knowledge-based organizations are problem-solving schemes that remain particulars involving to a problem state in knowledge base for investigation and removal of interloper (27). Knowledge base stores data particulars and measures in form of composite organizations for exploitation and future calculations and problem resolving. A technique for constructing knowledge base and applies appraisal scheme for system safeguarding (28). Centralized environments in clustered related approaches are more possibility to supervise routing and congestion in system. Nodes are assembled together to form clusters, every cluster is supervise by a node as CH (29). CHs relays with base station about paths event from nodes either direct or multi hop structure. CHs supervise activities and events made by nodes in clusters (30). CHs are elected to gain duration of nodes and continuation entire operations for extensive duration and comparison with proposed methodology (31).

Research work is organized as sections 2 illustrate related work. Irregular set tactic based malicious node recognition by information classification in section 3. Simulation Outcome and Investigation are demonstrated in section 4. Finally section 5 concluded research work and future work are designed.

Proposed Methodology

Three energy intensity mobile sensor nodes are organized as,

(i) Regular mobile node

(ii) Intermediary mobile node and

(iii) Superior mobile nodes.

For these three categories of sensor mobile nodes are classified based on behavior of nodes as

better, average, inferior utilizing irregular set tactic.

Working process

Implementation of proposed tactic follows,

a. Proposed network tactic consists of BS with heterogeneous system and diverse sensor nodes. Broadcasting factors are similar to routing protocols in MWSNs. Energy intensity of mobile nodes are established.

b. Energy level of entire mobile nodes calculated, if energy level is empty node is dead and entire system is also dead. Network cannot function otherwise go to setup and steady condition state.

c. Information classification to identify malicious mobile node utilizing irregular set tactic.

Set-up State

CH is determined in Set-up State. Constraints as remaining and opening energy are measured in a proportion of $REM_{eng}/Open_{eng}$ in threshold calculation formula equation 9-10. Remoteness constraint is calculated equivalent way by proportion of remoteness of node from base station and average remoteness of entire nodes from base station $R_{remote}(i)/AR_{remote}$ (equation 1-2). Total numbers of nearby sensor nodes are signify as TNS.

i. Possibility is evaluated for entire sensor nodes. Regular mobile node, intermediary mobile node and superior mobile nodes will have diverse probabilities due to diverse energy levels. Threshold is estimated for every category of sensor nodes.

ii. In corresponding an arbitrary number $\mathbf{A_n}$ is created. $\mathbf{A_n}$ value is evaluated for entire sensor node in network and contrast with threshold. If $\mathbf{A_n}$<evaluated threshold that node takes responsibility of CH otherwise cluster member node.

Selecting CH

Selecting CH is evaluated by arithmetical model. $R_{remote}(i)$ is node remoteness from BS. AR_{remote} is average remoteness of entire sensor nodes among BS. Selecting CH follows equations,

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

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

When

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

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

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

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

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

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

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

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

$$T_{norm}= P_{norm}/ (1-P_{norm}(\text{cmod}(1/P_{norm})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_s\text{div}(1/P_{norm})*(1-REM_{eng}*Open_{eng}*NM \quad \ldots[9]$$

$$T_{inter}= P_{inter}/ (1-P_{inter}(\text{cmod}(1/P_{inter})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_s\text{div}(1/P_{inter})*(1-REM_{eng}*Open_{eng}*NM \quad \ldots[10]$$

$$T_{advance}= P_{inter}/ (1-P_{advance}(\text{cmod}(1/P_{advance})))*(R_{remote}(i)/AR_{remote})*((REM_{eng}/Open_{eng})+(c_s\text{div}(1/P_{advance})*(1-REM_{eng}*Open_{eng}*NM \quad \ldots[11]$$

From equations 3-8 possibilities of regular, intermediary and superior mobile nodes are evaluated. Thresholds are evaluated from equations 9-11 for regular, intermediary and superior mobile nodes. Thresholds are contrasted with arbitrary number of entire nodes in system. For a particular node arbitrary number is below threshold such node is elected as CH superior node and subsequent threshold nodes are elected as intermediary nodes remaining nodes are as regular mobile nodes.

Steady Condition State

Data broadcasting is done in this state while data relaying following procedures are considered.

i. After selection of CH evaluate average remoteness among entire nodes from BS. Data relaying will based on average remoteness either in multi or single hop.

ii. Subsequently remoteness among CH and BS are evaluated. If average remoteness is large then CH relays data to nearby CH or relays straightforwardly to BS.

Malicious Node Identification

Averages of relaying rate are measured to categorize nodes related with resolution system. Nodes are categorized based on distinctiveness of every mobile node good or malicious. To categorize malicious movable nodes in system irregular set tactic used and dissimilar simulation are measured for divergent velocity. Malicious movable nodes are recognized and eradicate from route entry table in network. Update route entry table for routing data. Following process recognize malicious movable nodes in system. Receive

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

E2E delay

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 with 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

Relaying Metrics of mobile Node

Route entry table accumulates entire routes from source to target mobile node and circumvent unnecessary route innovation procedure. Route innovation tactic in on-demand routing tactics is extreme expensive in delay, energy and bandwidth utilization of network because of flooding cause extensive delay before relaying first packet. Performance of methodologies depends on proficient accomplishment of route entry table. When an unacceptable path is used for relaying data additional traffic arises and delays in routing are deserved to determine busted links. Eliminating route entry after a short Time-to-Live (TTL) is one strategy for reducing the consequences of an unsatisfactory path. Small suitable routes are discarded if TTL is too long, and massive routing delays and traffic may result from new route discovery. Paths are accumulated in route entry table to circumvent redundant route innovation for repeatedly used routes.

Construct simulation network consists of sensor mobile nodes. Metrics for mobile nodes that are calculated based on the performance of portable nodes. The performance of mobile nodes was assessed using broadcasting data.

Data deliverance proportion

Data deliverance proportion represents percentage among amount packets transmitted from application layer and amount of packets really obtained at target nodes.

E2E delay

E2E is average performance among mobile nodes in system. Sources and target nodes are occupied.

Throughput

Measure of booming data deliverance over complete simulation. It is premeditated by separating entire packets accepted by entire simulation procedure.

Plummet packets

Undelivered packets to target mobile node broadcasted from mobile sources.

Fault rate

Data packet produced separated by obtained packet in target node.

Duration

Relaying metrics of sensor mobile nodes is premeditated with diverse velocity like 5,10,15,20 and 25ms. Evaluated for five diverse nodes are recorded in table 1- 5.

Table 1: 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 2: 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 3: 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 4: 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 5: 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 6: 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

Information classification of irregular set tactic

Irregular set tactic

Irregular set tactic projected in 1982 by Pawlak is arithmetical tool which compacts with indistinctness and improbability. Process and conception are defined related with imperceptibility relation. In irregular set tactic information placed in table every event or object or entity is characterized in row and trait considered for element characterized in column thus information table is generated for classifying information. Entire elements set as universe is applied to selected trait to enhance effectiveness in originated rules. In Information classification elements contains similar value for every trait are imperceptible. Similar values of resolution traits are associate sets of universe as conception. An optimistic constituent is element of universe conception. Every conception maximum union elementary set in conception is lesser estimation and minimum union elementary set in conception is higher estimation of conception which is not constituent of lesser estimation is border area. It offers constructive information regarding responsibility of exacting traits and their associate sets and organizes information hidden by IF-THEN resolution principle. Set is irregular if border area is occupied otherwise crispy if border area is vacant.

Information Classification

Information classification analyzed as table rows in signifies object and columns signifies traits. Information classification is couple C=(U,T) where U is finite object of nonempty set in universe and T is finite traits of occupied set for t: $U \rightarrow E_t$ where $t \in T$, set E_t is evaluation set. Information classification enhanced by enclosure of resolution characteristics and information classifications as resolution structure. Resolution structure is information classification of S= (U,T,U{s}), where $s \notin T$. Resolution characteristics and elements in T are situation traits. Usually traits in resolution obtains two or multi probable values. Resolution classification articulates approximately entire information concerning representation. Information table contains similar or imperceptible objects signify numerous instance and other traits redundant is expressed in equation 12.

$SR(M) = \{(Y,Y') \in U^2 \mid \forall_t \in M\ q(y) = q(y')\}$ … [12]

Where SR(M)-similarity relation

M-imperceptibility relation

Irregular set tactic examination performed utilizing inferior and superior estimations shown below ,

Inferior estimation

$M^* Y = \{Y \in U : M(Y) \subseteq Y\}$ … [13]

Superior estimation

$M^* Y = \{Y \in U : M(Y) \cap Y \neq \phi\}$ … [14]

Where $M \subseteq T$ and $Y \subseteq U$.

Estimation Y by utilizing Information restricted in M by constructing inferior and superior estimations evaluated in equation 13 and 14. Granulity of information irregular set tactic sets unable distinguish with accessible information with entire rough irregular set tactic set connect with two crispy as inferior and superior estimations. Inferior estimation sets contains entire elements belongs to set. Dissimilarity among inferior and superior estimations is border area and irregular set tactic contain occupied set border area. Irregular set tactic differentiate numerically in equation 15.

$\alpha_M(Y) = |M^* Y| / |M^* Y|$ … [15]

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

if $\alpha_M(Y) = 1$,

Then set Y is crispy reverence to M

if $\alpha_M(Y) < 1$,

Table 7: 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

Table 8: 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

Then set Y is irregular reverence to M.

Some associate sets of restricted trait which safeguards portioning of universe and that associate sets as least reductions. That reductions can evaluated with imperceptibility matrix in equation 16 as,

X_{xy}= {a∈A| a(k_i) ≠a(k_j)} for x,y=1……n

a^*_1…….a^*_m =Λ{V C^*_{xy}|1≤y≤x≤n,X_{xy}≠Ø ...[16]

where X^*ij={a^*|a∈Xij}. Determine the consequence of estimated reduction and result on information set after eliminating meticulous trait by equation 17

∝(L,M)=1−γ(L− {α} ,M/γ (L,M)) ...[17]

Information classification is signifies in Table 7. Where event or object or entity is characterized in row and trait considered for element characterized in column.

Develop IF-THEN resolution policy from common values of entire nodes related with relaying record executes with diverse velocity.

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 8 illustrates categorization of diverse sensor mobile nodes and B indicates big, A indicates average and I indicate inferior. Above policy are to categorize nodes activities as fine or malicious. If Data deliverance proportion = big/average, E2E delay=inferior, Throughput= big, Plummet packets = inferior/average, Fault Rate = inferior/average, Duration= big/average then resolution= fine. Else if Data deliverance proportion= inferior, E2E delay= big, Throughput= inferior, Plummet packets = big, Fault Rate = big, Duration= inferior then resolution= malicious.

Examination of Data utilizing ISES

ISES (Irregular Set Examination System) utilized to acquire resolution policy and apply policy to identify malicious sensor mobile nodes in network. ISES examine table information with techniques and procedures in irregular sets. Following steps involved proposed tactic to implement and identify mobile malicious nodes.

Process:

1. Attach information to ISES.
2. Evaluate Reduct.
3. Develop Resolution policy.
4. Utilize categorizer as Resolution trees to discover from exercising information set.
5. Construct uncertainty matrix.
6. Utilize resultant resolution policy to identify malicious mobile nodes category.

Results and Discussion

Simulations passed out in NS2. Simulation atmosphere contains six sensor mobile nodes located consistently and outline a mobile atmospheric network regarding 1000 x 1000 meters region for simulation time of 1200 seconds. For testing in this research work paper Constant Bit Rate (CBR) constant bit rate is utilized. Mobility representations were produced by utilizing BonMotion tool with least velocity of5m/s and highest velocity of 25m/s are represented in Table 9 simulation atmosphere as,

Table 9: Simulation Factors

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

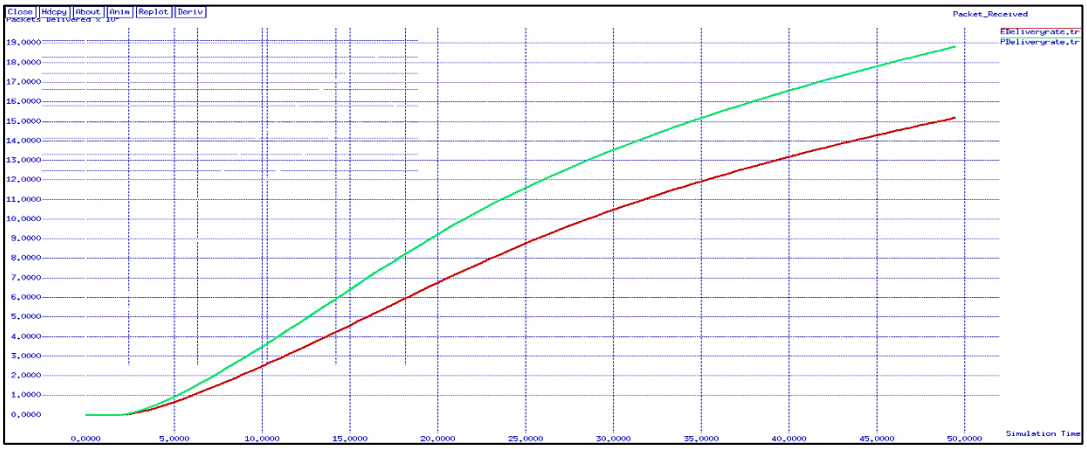

Figure 1: Packet deliverance versus Simulation Time of mobile sensor node

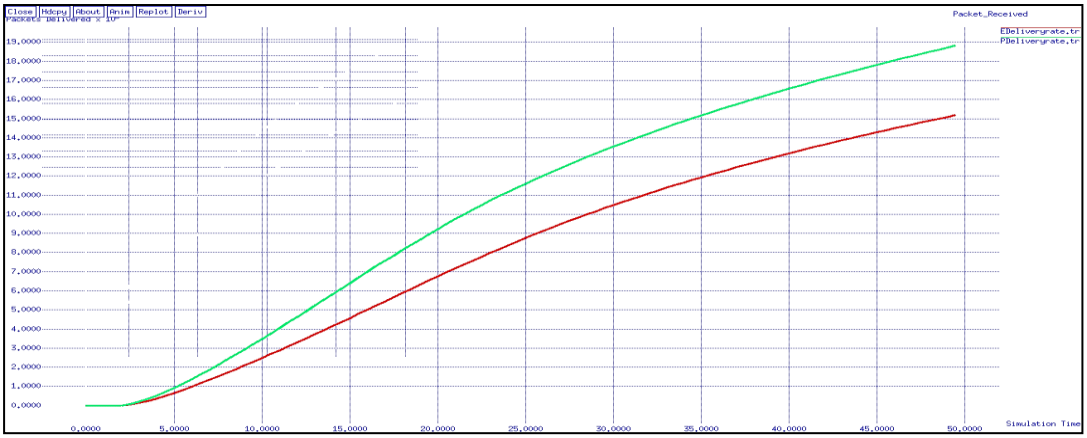

Figure 2: Plummet packets versus Simulation Time of mobile sensor nodes

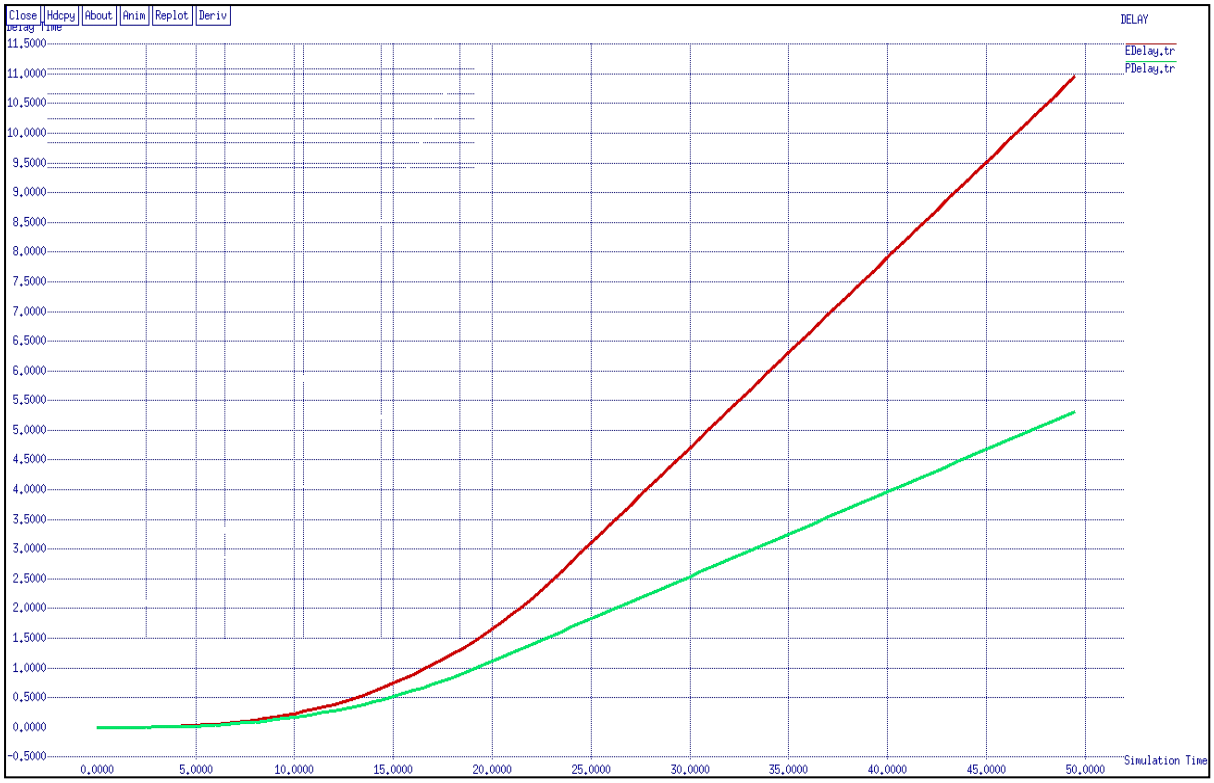

Figure 3: E2E Delay in mobile sensor nodes.

Figure 4: Proficient Energy to Increase duration of Network

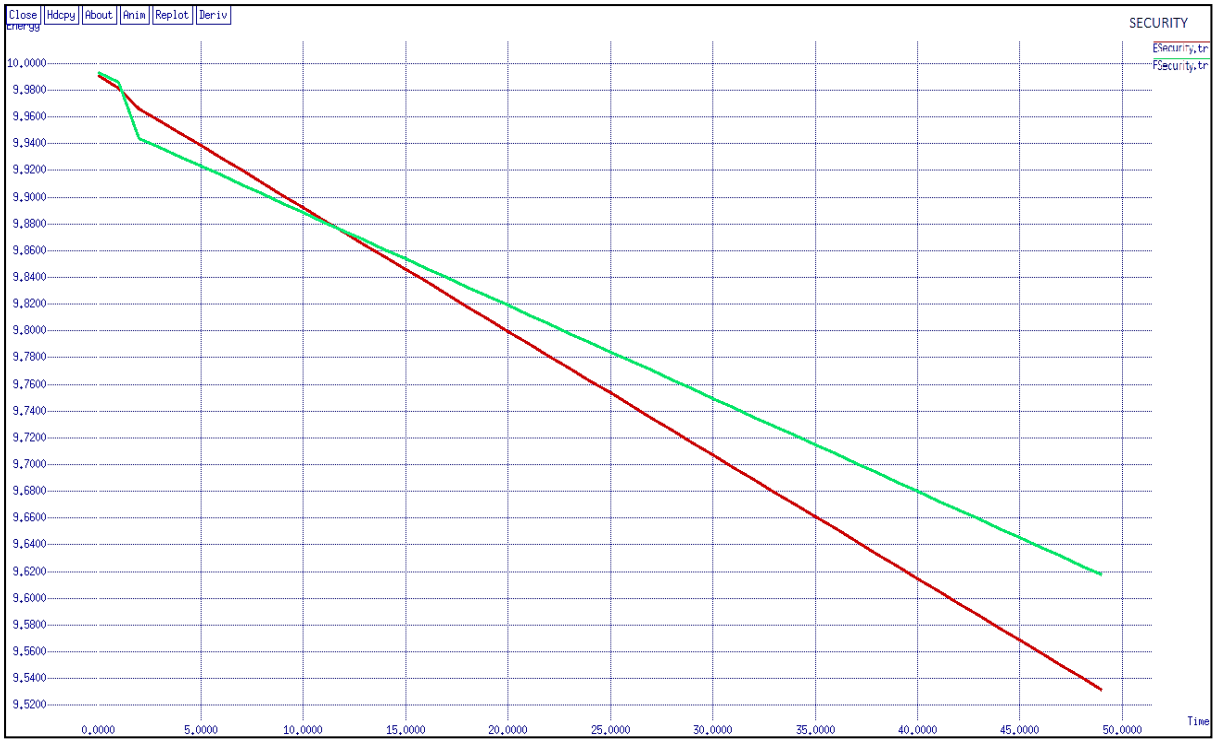

Figure 5: Increase of Security level in mobile nodes.

In Figure 1, the suggested tactic's packet delivery is compared to the Cross-layer-based Opportunistic Routing Protocol (CORP) methodologies packet delivery. In comparison to CORP, the range of packets sent to BS for irregular set strategy routing protocol is higher. The proposed approach is shown in green, whereas the current method is shown in red. It is clear that the proposed approach's packet delivery proportion is superior to the current CORP.

In Figure 2, the proposed method's plummet packets ratio is compared to the CORP methodology's plummet packets ratio. When compared to CORP, the quantity of Plummet packets is lower for irregular set strategy routing protocol. This is due to the fact that the irregular set tactic contains information on the location of the remote sensor node. Unsuccessful information delivery over a broadcasting channel is known as plummet packets. This is the amount of data lost because the target sensor is unable to receive data. The proposed method is depicted in green, while the CORP approach is depicted in red. It's reasonable that the proposed approach's packet loss is lower than the present way.

In Figure 3, the proposed tactic's E2E latency is compared to the CORP methodology's E2E delay. In comparison to CORP, E2E is reduced while using an irregular set strategy routing approach. Because the irregular set technique incorporates routing information, this is the case. As a result, the information was supplied on time. The green line represents the suggested method, while the red line represents the existing methodology. It's understandable that the proposed technique takes less time than the CORP technique.

In figure 4, the proficient energy of the proposed methodology is compared to the proficient energy of the CORP technique. To reduce reclustering, the energy efficiency of sensor nodes is estimated. In mobile sensor nodes and CHs, the irregular set approach has a higher energy level. The green line represents the proposed system, while the red line represents the existing system. It is understandable that the proposed technique has a higher energy level than the CORP system.

In figure 5, the suggested method's security is compared to the CORP technique's security level. When compared to CORP, the irregular set tactic method improves security in BS, CHs, and mobile sensor nodes. This is due to the irregular set tactic's usage of mobility-based intrusion detection in BS, CHs, and mobile sensor nodes, which improves network security. The CORP energy efficient reliable routing algorithm simply assesses energy efficiency and provides less

information security. The green line denotes a proposed project, while the red line denotes an existing scheme. It is understandable that the suggested scheme's security level is higher than that of CORP.

Conclusion

Security in MSWN is a demanding assignment for researchers due to mobility environment and resources limitation. Route entry table in system recognize malicious sensor mobile node related with relaying record. Entire mobile nodes in network preserve route entry table and relaying record of its nearby mobile nodes. According to its relaying record sensor mobile nodes are categorized utilizing irregular set theory to recognize mobile nodes are fine or malicious. Irregular set tactics assist to eradicate redundant traits and produces smallest traits set as reduction by safeguarding separation of universe and produce resolution policy. To originate resolution policy for categorize sensor mobile nodes. If generate route contains malicious mobile node data transmitter selects diverse shortest route for relaying. Thus effectively distinguish event plummeting mobile nodes from network. Linkage breakdown easily identified use of route entry table in system. Little recompense with this methodology is fake recognition rate and transparency on system is diminished. Simulation result indicates that data deliverance proportion, throughput, security, remaining energy and E2E delay enhanced than existing methodologies. In future implementation can perform in neural network, cross models and fuzzy set to recognize malicious sensor mobile nodes in network.

Abbreviations

BS: Base Station
CBR: Constant Bit Rate
CH: Cluster Head
CORP: Cross-layer-based Opportunistic Routing Protocol
DSR: Dynamic Source Routing
E2E: End-to-End
IDS: Intrusion Detection Systems
ISES: Irregular Set Examination System
LEACH: Low-Energy Adaptive-Clustering Hierarchy
LEACH-C: Low-Energy Adaptive-Clustering Hierarchy-C
MANET: Mobile Ad hoc Network
MWSN: Mobile Wireless Sensor Network
OLSR: Link State Routing
SA: Simulated Annealing
TTL: Time-to-Live

Acknowledgement

Nil

Author contributions

All the contributed in writing, concept, methodologies, implementation, reviewing and Analyzing the manuscript.

Conflict of interest

The authors declare that there is no conflict of interest.

Ethics approval

This article does not contain any studies involving human participants performed by any of the authors.

Funding

This article does not contain any funding.

References

1. Rajesh D, Giji Kiruba D, Ramesh D. Energy Proficient Secure Clustered Protocol in Mobile Wireless Sensor Network Utilizing Blue Brain Technology. Indian Journal of Information Sources and Services. 2023;13(2): 30–38.
2. Amin Shahraki, Amir Taherkordi, Øystein Haugen, Frank Eliassen, Clustering objectives in wireless sensor networks: A survey and research direction analysis. Computer Networks. 2020; 180(1):107376.
3. Priyadarshi R, Gupta, B, Anurag A. Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues. J Supercomput. 2020; 76: 7333–7373.
4. Rajesh D, Jaya T. Energy competent cluster-based secured CH routing EC2SR protocol for mobile wireless sensor network. Concurrency Computat Pract Exper. 2022; 34(1):e6525.
5. Rajesh D, Kiruba Giji D. Energy Efficient Secured CH Clustered Routing (E 2SCR) in Smart Dust Network. Journal of Intelligent and Fuzzy Systems. 2022; 43(6): 8349-8357.
6. Rajesh D. Energy-Resourceful Routing by Fuzzy Based Secured CH Clustering for Smart Dust. International Journal of Electrical and Electronics Research. 2022; 10(3):659–663.
7. Dennison R, Dennison R, Dasebenezer GK, Chinnathurai ES. Enhancing lifespan and energy efficiency in mobile smart dust networks.

Ingénierie des Systèmes d'Information. 2023; 28(5): 1317-1323.
8. Serhani A, Naja, N, Jamali A. AQ-Routing: mobility-, stability-aware adaptive routing protocol for data routing in MANET–IoT systems. Cluster Computing. 2020;23:13–27.
9. Rajesh D, Kiruba D., A Comparative Study on Energy Efficient Secured Clustered Approaches for IOT Based MWSN, Suranaree Journal of Science and Technology, 2022; 29(4):1-18.
10. Rajesh D, Jaya T. A Mathematical Model for Energy Efficient Secured CH Clustering Protocol for Mobile Wireless Sensor Network. Wireless Personal Communications. 2020; 112(1): 421-438.
11. Singh CE, S. M. Vigila SMC. Woa-dnn for intelligent intrusion detection and classification in manet services. Intelligent Automation and Soft Computing. 2023; 35(2): 1737–1751.
12. Edwin Singh C, Maria Celestin Vigila S. Fuzzy based intrusion detection system in MANET. Measurement: Sensors. 2023; 26: 100578.
13. Giji Kiruba Dasebenezer, Benita Joselin, TSO Clustered Protocol to Extend Lifetime of IoT Based Mobile Wireless Sensor Networks. The International Arab Journal of Information Technology (IAJIT). 2023; 20(04): 559 - 566.
14. Jasim AA, Idris MYI, Razalli Bin Azzuhri S, Issa NR, Rahman MT, Khyasudeen MFb. Energy-Efficient Wireless Sensor Network with an Unequal Clustering Protocol Based on a Balanced Energy Method (EEUCB), Sensors, 2021; 21(3): 784.
15. Kiruba DG, Benita J. A Survey of Secured Cluster Head: SCH based Routing Scheme for IOT based Mobile Wireless Sensor Network. ECS Transactions. 2022;107(1): 16725–16745.
16. Kiruba DG, Benitha J. Fuzzy based energy proficient secure clustered routing (FEPSRC) for IOT-MWSN. Journal of Intelligent and Fuzzy Systems. 2022; 43(6):7633–7645.
17. Giji Kiruba, Benita. Energy capable clustering method for extend the duration of IoT based mobile wireless sensor network with remote nodes, Energy Harvesting and Systems, 2021;8(1): 55-61.
18. Pal R, Subash Yadav, Rishabh Karnwal, Aarti . "EEWC: energy-efficient weighted clustering method based on genetic algorithm for HWSNs". Complex Intell Syst. 2020; 6: 391–400.
19. Rajesh D, Kiruba DG. A probability based energy competent cluster based secured ch selection routing EC2SR protocol for smart dust. Peer-to-Peer Netw Appl. 2021; 14: 1976–1987.
20. Buwen Cao, Shuguang Deng, Hua Qin and Yue Tan. A novel method of mobility-based clustering protocol in software defined sensor network. J Wireless Com Network. 2021; 99.
21. Rajesh D, Rajanna GS. CSCRT protocol with energy efficient secured CH clustering for smart dust network using quantum key distribution. International Journal of Safety and Security Engineering. 2022; 12(4): 441-448.
22. Mohit Jain MB. A Rough Set based Approach to Classify Node Behavior in Mobile Adhoc Networks. Journal of Mathematics and Computer Science. 2014; 11: 64-78.
23. Anshu Chauhan D. Detection of Packet Dropping Nodes in MANET using DSR Protocol. International Journal of Computer Applications. 2015; 123(7): 0975-8887.
24. Mehmood A, Khanan A, Mohamed AHHM, Song H. ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET'. IEEE Access. 2018;6.
25. Rajesh D, Jaya T. Exploration on Cluster Related Energy Proficient Routing in Mobile Wireless Sensor Network. International Journal of Innovative Technology and Exploring Engineering. 2019; 8(4): 93-97.
26. Zhen-Zhong Hu, Shuo Leng, Jia-Rui Lin, Sun-Wei Li, Ya-Qi Xiao. Knowledge Extraction and Discovery Based on BIM: A Critical Review and Future Directions. Arch Computat Methods Eng. 2021;9:335-356.
27. Umar M M, Mehmood A, Song H. SeCRoP: Secure CH centered multi-hop routing protocol for mobile ad hoc networks. Secur Commun Netw. 2016; 9(16): 3378-3387.
28. Balasubramanian Muthusenthil, Hyunsung Kim, VB Surya Prasath. Location Verification Technique for Cluster Based Geographical Routing in MANET, Informatica. 2020;31(1): 113-130.
29. Wenjie Zhang, Dezhi Han, Kuan-Ching Li, Francisco Isidro Massetto. Wireless sensor network intrusion detection system based on MK-ELM. Soft Comput. 2020; 24: 12361–12374.
30. Sharma N, Gupta V. A Framework for Wireless Sensor Network Optimization Using Fuzzy-Based Fractal Clustering to Enhance Energy Efficiency, Journal of Circuits, Systems and Computers. 2022; 31(13): 2250223.
31. Shanmugam R, Kaliaperumal B. An energy-efficient clustering and cross-layer-based opportunistic routing protocol (CORP) for wireless sensor network. Int J Commun Syst. 2021; 34:e4752.