International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Real Time Node Identity Based Multi Algorithm Framework for Enhancing MANET Performance

S. Gnanavel[1], S. Muruganandam[2], G. Balamurugan[3*], N. Duraimurugan[4]

Submitted: 07/05/2023 **Revised**: 18/07/2023 **Accepted**: 07/08/2023

Abstract: In Mobile Ad-hoc Network security in data transmission and efficient power utilizations are two major concerns. Maintaining the reliability during the information transference in routing is another major issue, due to the existence of routing threats in the networks. The stability of the networks is reduced. The reliable and energy efficient route is identified to deliver the information packets from origin to target point. This paper proposes a Real Time Node Identity Based Multi Algorithm Framework that enhances the performance of a network. The energy effective cluster head searching algorithm is used to minimize the power utilization of the networks. The selection of cluster header is based on various trust factors of a node; the node trust is measured by various quality attributes of a node such as mobility of a node, energy consumption of a node, degree of connectivity of a node and reliability value of a node. The measurements of all these attributes are estimated for all nodes in the network. The reliability value of a node is estimated by the cumulative value of all these attributes. The reliability value is used for identifying the suspicious nodes in the network. The proposed method RTNIDBMAF introduces four algorithms, the first algorithm supports to measure the energy efficient clusters header node. This efficient cluster header node will determine the optimum path in the network. Second algorithms are used to perform malicious node detection and removal based on the value of vulnerability index. The reliability in data transmission is improved through malicious node detection and removal methods. Third algorithm is used to perform energy optimized routing based on energy consumption of a node. The fourth algorithm is used to perform secure data transmission in routing by applying public key cryptographic methods. The efficiency of the developed algorithm is measured by the simulation results. The proposed algorithms enhance the Quality of Services in Mobile Ad-hoc networks while comparing with existing methods and the results are displayed in the graph.

Keywords: *wireless sensor networks, digital motion processor, machine learning, Routing Protocol for Low-Power and lossy Networks*

1. Introduction

The wireless sensor networks (WSN) is a widely used internet, it is an infrastructure-less network, and this kind of networks can be easily deployed. It includes sensors with closed setups, such as limited power supply and little storage capacity [1]. Cluster-based WSN is a feasible solution for preserving energy. A digital motion processor (DMP) is used by smart sensors to extract significant details from the data they capture about their environment [2]. Multi-hop communication was used to convey this data to the cluster head, which then sent it to the main base station. A gateway is used to send this error-free data to the distant user [3]. An unsecure environment is created in WSN as a result of the routing path's insecurity. The universal attack to destroy network stability is a routing attack [4]. Numerous routing attacks exist, including the sinkhole, black hole, and Sybil attack. Finding and removing rerouting intrusions from the entire network is a crucial issue [5].

A confidential data transmission system is necessary to guarantee the network's accessibility, authenticity, and privacy while using the least amount of power sources possible. With a minimum of energy usage, machine learning (ML) determined methods offer a reliable and ideal way to identify and eliminate rerouting threats [6].ML can be supervised, unsupervised, or reinforced learning. In Section 2, the researchers present a number of ML-based methods. These solutions do not perform well in complex real-time systems since they are based on static data [7]. In this article, an innovative strategy is suggested for enhancing network security while using the least amount of energy possible. By minimizing anomalies, it improves the network's dependability. Identify the minimum Routing span calculated on Trust Values, Intruders Monitoring and elimination Methods are the two sections of the suggested method. The routing settings are then subjected to machine learning after the cluster header is chosen using trust value. It reduces the energy used for data transmission while routing. Second, the transmitting

[1]*Associate Professor, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur Campus-603203, Chengalpattu, Tamil Nadu, India.*
[2]*Assistant Professor, Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai – 600 123, Tamil Nadu, India*
[3*]*Assistant Professor, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur Campus-603203, Chengalpattu, Tamil Nadu, India.*
https://orcid.org/0000-0002-5676-5235
[4]*Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, Tamil Nadu, India*
** Corresponding Author Email: balamurg1@srmist.edu.in*

threats using node movement systems are identified and eliminated using the Intrusion Detection System (IDS) method. Section 2 of the paper discusses the relevant work. The recommended work is described in Section 3, Flow chart of proposed model is identified in Section 4, and The Simulation outputs are presented in Fig.5.0 The conclusion is displayed in Section 6.

2. Related Work

The Two important performance criteria in WSN are security and energy efficiency [8]. Researchers in networking provided a number of solutions; however they only function with static data [9]. The network layer is where the sinkhole attack happens. An IDS method is provided to find the intrusive party throughout the internet [10]. By applying measurements such as packet obtained, packets delivered, and ratio of intrusion, the LEACH protocol was utilized to increase the efficiency of routing operations across the system [11]. The specific taxonomy of the Denial-of-Service attack has received a lot of attention from researchers [12]. For each attack, an exact detection and prevention mechanism was developed in order to evaluate the benefits and drawbacks of every strategy. Using the Cooja simulator, the Routing Protocol for Low-Power and Lossy Networks (RPL) was utilised to prevent routing collision. These methods are restricted to a static dataset and made inefficient in practical situations [13]. The suggested approach uses ML to fix this problem. In order to explore the significance of ML algorithms in every one of these difficulties, such as transmitting the data, positioning, events recognizing, and energy accuracy, a specific ML model was applied to the various WSN issues [14]. In the dynamic setting of the WSN, ML outperformed. Another study provides a novel IDS approach to identify and eliminate the hybrid anomaly [15]. In process of increasing the performance of suggested approach as it was simulated using the opnet network simulator, K-means unsupervised ML was utilized to the Intrusion Detection method, Data sent and received metrics, latency, and other performance indicators were examined [16]. The clustering method increased energy efficiency. The clustering approach was used by the algorithm to split the routing problem into two halves. Two levels of routing were used: transmission of data packets to cluster circles and transmission of data packets to clusters. At the cluster ring level, reinforcement-based understanding was used, and a greedy technique was used for routing at the cluster level [17]. By improving the network's scalability and energy efficiency, this strategy offered the optimum routing solution. A Naive Bayes approach was used to address the problem of choosing the best cluster head, finding the cluster head with the least amount of overhead. It produced the most durable network outcome [18]. Routing attacks compromise the data's integrity. SVM ML was applied to address and fix this problem. Three uploaded data characteristics, including voltage, temperature, and humidity, were obtained from network traffic. This input data was divided into clusters based on density. [19]. Accuracy was evaluated using the density-based spatial clustering of applications with noise (DBSCAN) technique [20]. It observed that the low-density area had behaved abnormally and had been eliminated from the network data [21]. The challenge of outlier detection was addressed using empirical techniques [22]. The first technique combines a sliding window-based strategy with least-square SVM. Principal Component Analysis (PCA) was employed in the second method [23]. The problem with outliers in WSN was solved by implementing these two strategies. Automated variation identification relies on integrating boundary data and cloud data evaluation was used to solve the heterogeneous WSN anomaly detection problem [24]. In order to accurately discover deviations through online prediction with the least amount of energy consumption and the lowest possible number of false alarms, the Online Locally Weighted Projection Regression (OLWPR) method was suggested. The first phase used data compression. Subsequently, LWPR was used for prediction [25]. In addition, a dynamic threshold was used to identify abnormal data. Different solutions were recently made up by researchers [26]. The optimum routing solution in terms of security and energy efficiency is still required. Additionally, a method for effectively dealing with networks' dynamic behaviour needs to be investigated [27]. The researchers had recommended several methods, Still there is a requirement for the desirable approach to improve security and energy accuracy while rerouting data from origin to endpoint, also a method which will effectively handle the dynamic nature of networks need to be proposed.

3. Proposed System

The recommended system in Fig 1. proposes a reliable and efficient routing technique that functions with two phases; phase 1 defines energy efficient shorter routing routes based on reliability value and Phase 2 defines malicious node detection and removal methods. This method improves the security and energy accuracy in routing throughout data communication. The Clustering oriented wireless networks are adopted to reduce the consumption of energy. The sensors collect data from its sensation fields and produce the clustering. The optimum cluster head is chosen by applying decision-tree methodology. Security is improved using detection and eradication of intrusion methods. Routing attacks are identified using a threshold value, and the mobility model is used to eliminate these attacks.

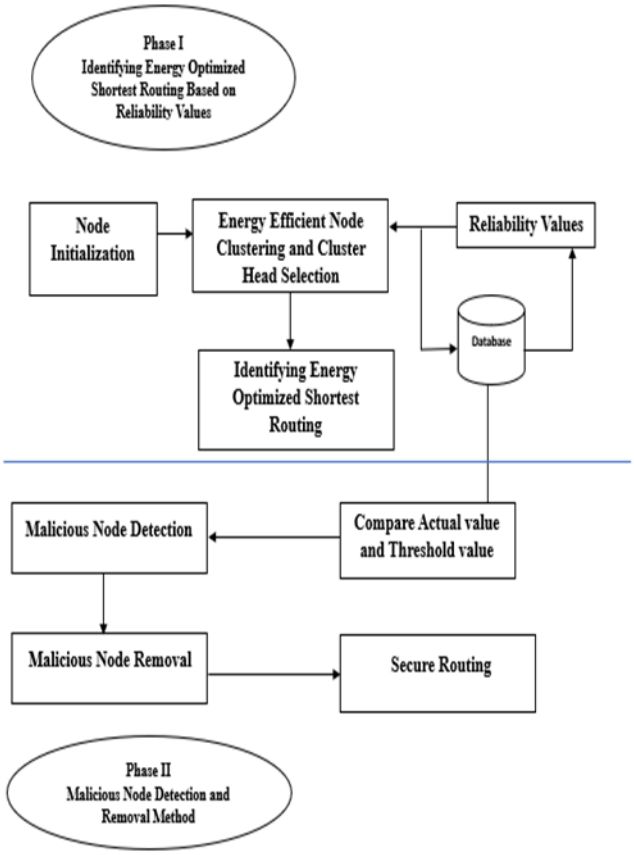

Fig 1. Proposed Architecture Model

2.1 Computing Shortest Routing Path Using Reliability Values

The Sensor nodes are spread over the wireless networks using networks simulators. The data communications between the origin and the target node in wireless networks is represented in Fig 2 The nodes N1, N2, N3 are sensors node that forwards observed data to the cluster Head. In the regular flow of data transmission, no malicious nodes are identified. If the suspicious nodes are presented in the structure, then it forwards the fake data to the cluster head node, and the cluster head makes the false routing path decision. In this contest we need to secure data in the network. The Security in the routing path is implemented by applying the computation of node reliability mechanism. The reliability value of the node is measured by using specific attributes retained in a database, The some of the attributes used are, node distance from the cluster head, Mobility of a node, residual energy.

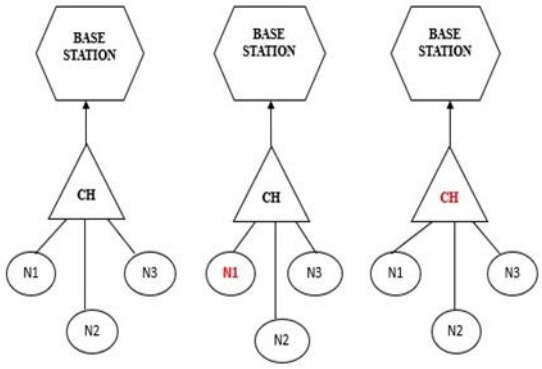

Fig 2. (a) Regular Flows(b) Attacks in Node N1 (c) Attacks in Cluster Head (CH) Node

2.1.1 Node Reliability Method

The node reliability value of all nodes in the networks is predicted by the interaction of direct and indirect node reliability calculation. The direct reliability estimation is determined on node self-analysis and it is computed in specific time duration as described in the subsequent example.

Ratio of Accepted Packets:

If the origin node A sends the data packets to the target node B in the communication network. The Obtained packet ratio is measured by the number of acknowledgements (ACK) sent back by the target node B to the origin node A.

Ratio of Received Packet =

$$\frac{The\ Number\ of\ Packets\ sent\ by\ the\ source\ Node\ A}{The\ Number\ of\ Acknownlodgement\ received\ by\ Node\ A} \quad (1)$$

This ratio will always equal the quantity of packet sent by the source Node A, if anything differences in the ratio will observe the behaviour of the Node B.

$$Receiver_{Pkt(i,i+1)}(t) = \frac{Receiver_{pkt(i,i+1)}(t) - Receiver_{pkt(i,i+1)}(t-1)}{Receiver_{pkt(i,i+1)}(t) + Receiver_{pkt(i,i+1)}(t-1)} \quad (2)$$

This element restricts to routing attacks using the support of recipient acknowledgements analysis. In the similar method, the entire factors will be computed based on the reliability values of the networks. An indirect reliability value is measured by the suggestion of the third node, and that is generally the adjacent node of Node A and Node A+1, expressed as Node K . Reliability consists of transition properties. The indirect reliability value of $\mathbf{Reliability^{u}_{i,i+1}}$ from $\mathbf{Node_k}$ to $\mathbf{Node_{k+1}}$ is determined by the suggestion $\mathbf{Node_i}$ ($\mathbf{Node_i} \in \mathbf{Node_k}$, defined by the equation 2).

$$Reliability^{u}_{i,i+1} = \text{Reliability i,u} \quad X \quad \text{Reliability u,i+1} \quad (3)$$

Where $\mathbf{Reliability}^{\mathbf{u}}_{\mathbf{i,i+1}}$ is the reliability value of node i to node u and Node u to Node i+1. Reliability i,u is the direct reliability value of Node i to the general adjacent Node u ,$\mathbf{Reliability}^{\mathbf{u}}_{\mathbf{i,i+1}}$. is the direct reliability values of the general neighboring node Nodeu to Nodeu+1. Subsequently all suggestions are not accurate. There is a need for finding invalid suggestions and eliminating those suggestions from the sum of all consolidated suggestions to find indirect Reliability more accurately. The Suggestions are elected by applying a threshold value. When a legitimate suggestion is higher than the threshold value, it will be explored as trusted suggestions. When the node has a high reputation, maximum weights are assigned to the node, and the particular route is suggested for involving the data transformation process. The weightage values are assigned in response to the reliability measure of the suggested to ignore the single suggestions. Maximum weight is allocated to the elected suggestion from referral sources having significant popularity.

Weight is computed by using equation

$$\text{Weight}_k = \frac{Reliability_{n,w}}{\sum_{w=1}^{j} Reliability_{n,w}} \quad (4)$$

where $\text{Reliability}_{n,w}$ is the proper reliability value of Node_n to the general adjacent node Node_v and j is the quantity of the selected suggestions. The indirect reliability value is identified as IND_Reliability (t) and computed by applying the formula

$$\text{IND\_Reliability (t)} = \sum_{w=1}^{j} \text{weight}_w * \text{Reliability}^{w}_{i,i+1}, w = 1,2,3, \ldots j \quad (5)$$

Where $\text{weight}_w$is the degree of $\text{Reliability}^{w}_{i,i+1}$

$Reliability^{w}_{i,i+1}$ Indicates the reliability value from Node_i to Node_{i+1} computed by the suggestion node Node_w.

Distance: The Distance can be computed by the Angle of Arrival (AOA) method,In this method, the angle at which the signal arrives at a receiving node is used to estimate the distance between two mobile nodes. It relies on the geometric relationship between the angle of arrival and the distance.

$$d = b / \tan(\theta) \quad (6)$$

Where:

b is the baseline distance between the two receiving nodes.

θ is the measured angle of arrival.

Mobility: It represents the rate of change of position and is typically calculated as the distance traversed by a mobile node per unit of time.

$$\text{Speed} = \text{Distance} / \text{Time} \quad (7)$$

For example, if the distance that a mobile node has travelled is measured in meters and the time taken is measured in seconds, the speed will be expressed in meters per second (m/s).

Estimating the remaining energy of a node:

$$\text{Remaining Energy} = \text{Initial Energy} - (\text{Energy Consumption Rate} * \text{Elapsed Time}) \quad (8)$$

The formula assumes a linear energy consumption model, where the energy consumption rate remains constant over time. The elapsed time represents the duration for which the node has been operational.

In this formula,

Initial Energy: Initial Energy refers to the total energy capacity or the energy level of the node when it started its operation.

Energy Consumption Rate: Rate at which the node consumes energy over time.

Elapsed Time: Elapsed Time represents the duration for which the node has been operational.

Reliability Value: It is a measure of a node's reliability in a network we can consider various factors to quantify it

$$\text{Reliability Value} = (w1 * A1) + (w2 * B2) + (w2 * C3) + (w2 * D4) \ldots + (wn * Fn) \quad (9)$$

In this formula,

A1, B2,C3,D4 ..., Fn represent individual factors that contribute to the Reliability value, and w1, w2, ..., wn are the corresponding weights assigned to each factor. The weights indicate the relative significance of each factor in assessing the overall Reliability Value.

Algorithm 1: Energy-Efficient Distributed Clustering

Input: Gathered sensor data: Network topology, Remaining energy of a node, Distance, Threshold Value

Output: Cluster formation

Step 1: Initialize the sensor nodes in the network

Step 2: Set the initial random node as Cluster Head

Step 3: Calculate the Distance, Mobility, Remaining Energy, by using the formula (6), (7),(8).

Step 4: Compute the Cumulative Reliability Value using the formula (9)

Step 5: Repeat the steps 3 and 4 for all nodes in the network

Step 6: Determine the node having maximum Cumulative Reliability Value

Step 7: Compare the maximum values and threshold values of sensors nodes

If Reliability values> threshold values

Set the node as Cluster Header

Else

No Cluster Header formation, Wait for the new nodes to join in the network and repeat the steps

Step 8: Update the routing path

Algorithm 2: Malicious Node Detection and Removal

Input: Gather data: Node, Vulnerability Index, Connectivity Information

Output: Detected compromised nodes, Remedial actions

Step 1: Initialize the list of detected intrusions and compromised nodes as empty

Step 2: Compute the vulnerability index value for all sensor node using the formula

Step 3: Repeat for each sensor node in the network

3.1 Analyze the sensor node data for anomalies or suspicious behaviors

Step 4: Compares the Trust value and threshold value

If Reliability values< Threshold Values

Add the node to the compromised node list

Step 5: If the list of compromised nodes as not empty, repeat the step 2

Step 6: Return the list of compromised nodes

Step 7: Isolate the compromised nodes in the network and update the routing path.

Algorithm 3: Energy Optimised Routing Algorithm

Input: Network topology and connectivity information, Residual energy, Energy consumption rates of data packets, No of data packets delivered.

Output: Selected Route for data transmission

Step 1: Initialize the routing table for all nodes in the network

Step2: Set the energy threshold for node selection

Step3: Repeat until destination is reached:

3.1 Calculate the energy-efficient route from the source to the destination:

3.2 For each neighbor node of the current node:

3.3 Calculate the energy cost of transmitting to the neighbor

Step4: Calculate the total energy consumption to reach the destination via the neighbour node

Step5: Update the routing table with the energy-efficient route if it provides a lower total energy consumption

Step6: Select the next hop based on the routing table:

6.1 Choose the neighbour node with the lowest total energy consumption

6.2 Update the current node to be the selected next hop

Step7: Return the selected route for data transmission

Algorithm 4: Public key-based cryptographic algorithm for secure routing

Input: Network topology and connectivity information, public key and Private key of a nodes, Data Packets to be transmitted

Output: Securely routed data packets

Step1: Initialize the routing table for all nodes in the network

Step 2: Set the initial route as an empty path

Step 3: Repeat until destination is reached:

3.1 Calculate the secure route from the source to the destination:

3.2 For each neighbour node of the current node:

3.3 Generate a session key for secure communication with the neighbour

3.4 Encrypt the data packet using the neighbour's public key

3.5 Append the encrypted data packet to the path and update the routing table

Step 4: Sign the path using the current node's private key

Step 5: Update the routing table with the secure route if it provides stronger security

guarantees

Step 6: Select the next hop based on the routing table:

6.1 Choose the neighbour node with the most secure route

6.2 Update the current node to be the selected next hop

Step 7: Return the securely routed data packets

4. Flowchart Model of Proposed Method

The recommended approach offers efficient communication while maintaining security and minimising energy. The Energy-Efficient Distributed Clustering algorithm supports to finding the shorter routing paths from source to destination nodes based on the computation of reliability value of a node. The Malicious node identification and elimination algorithm is used for detecting the intrusion node efficiently using the Threshold value. After elimination of malicious nodes, the routing path is free from attackers and it becomes the secure routing.

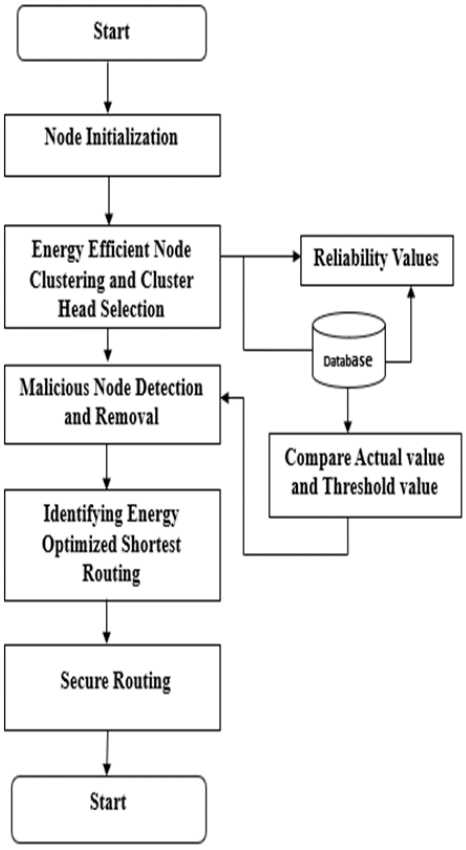

Fig.3. Flow Chart of Proposed Model

5. Simulation and Results

The recommended method is executed by using the NS2 simulator. For examinations,100 sensor nodes are deployed for developing networks with (200 × 200) m2 and initial power of a mobile node is 5J.

Table. 1. Simulation specifications

S.No	Factors	Quality
1	Network Area	200 × 200m^2
2	Quantity of Nodes	100
3	Movement	Random
4	Velocity	0-60 m/s
5	Simulation Period	600

5.1 Performance Analysis

5.1.1 Clustering Accuracy:

The level of accuracy in clustering for the proposed method is determined by the number of overlaps it generates for a specific number of network nodes.

Clustering Accuracy = $\frac{Number\ of\ Overlaps}{Total\ Number\ of\ Nodes}$

Table 2: Analysis on clustering quality

Accuracy of Clustering Analysis			
	50 Nodes	100 Nodes	200 Nodes
GCEEC	65	71	73
DBSCAN	68	73	79
K-WCA	71	74	81
CHFL	73	82	84
RTNIDBMAF	76	86	88

The accuracy of clustering is measured for various methods and the outcomes such evaluation is presented in detail in table 2. However, the recommended RTNIDBMAF has generated better clustering efficiency when compared to existing methods. The proposed RTNIDBMAF has produced 76%,86%,88% of clustering efficiency in the existence of 50 nodes,100 nodes and 200 nodes in the network which is greater than Gateway Clustering Energy-Efficient Centroid (GCEEC), Density-Based Spatial Clustering of Applications with Noise (DBSCAN) strategy, K-means weighted clustering algorithm(K-WCA), Cluster Head Fuzzy Logic (CHFL).

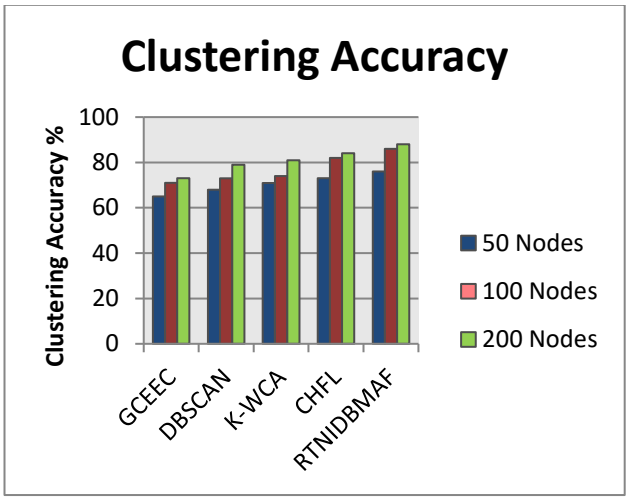

Fig. 4. Accuracy in Clustering Performance

The efficiency in node clustering is assessed by varied nodes in the network and displayed in Fig.4. The recommended RTNIDBMAF method produces better efficiency than GCEEC, DBSCAN, K-WCA and CHFL.

5.1.2 Accuracy of Malicious Node Detection:

The malicious node detection accuracy is measured by using this formula.

$$\text{Detection Efficiency} = \frac{\textit{Number of Malicious Nodes identified.}}{\textit{Total Number of Malicious Nodes in Network}}$$

Accuracy of Malicious Node Detection			
	50 des	100 Nodes	200 Nodes
PEACM	63	66	71
DCBM	66	71	73
RBIDT	71	74	76
MJRM	73	78	82
RTNIDBMAF	86	92	96

Table 3: Analysis on Malicious Node Identification performance

The Accuracy of malicious node detection is evaluated using several strategies and the results of such assessment are displayed in detail in table 3. However, the recommended RTNIDBMAF has generated better malicious node identification efficiency when contrasted to existence methods. The recommended RTNIDBMAF has developed 86%,92%,96% of detection efficiency in the existence of 50 nodes,100 nodes and 200 nodes in the system which is greater than Power Efficient Adaptive Clustering Method (PEACM), Decentralised Cluster Based Routing Method (DCBM) techniques, Reliability Based Intrusion Detection Techniques (RBIDT), Multiple Judge Reward Method (MJRM).

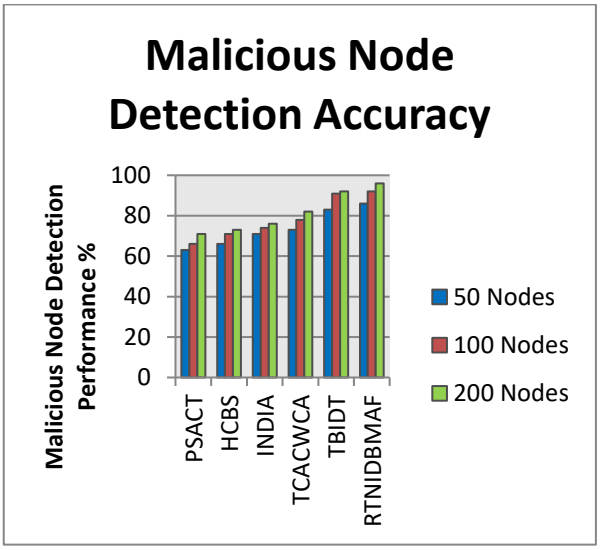

Fig.5. Malicious Node Detection Accuracy

5.1.3 Energy Consumption Analysis:

The Malicious node identification is analysed by various nodes in the structure and displayed in the fig.5. The suggested RTNIDBMAF method produces the maximum efficiency than PEACM, DCBM, RBIDT, MJRM.

The energy consumption analysis is measured by the formula

$$\text{Energy Consumption} = \frac{\text{Amount of Energy in Joules spent by the node}}{\text{Number of Transmission Performed}}$$

Performance Analysis of Malicious Nodes			
	50 Nodes	100 Nodes	200 Nodes
PEACM	67	71	78
DCBM	66	77	76
RBIDT	67	78	79
MJRM	59	64	78
RTNIDBMAF	52	56	61

Table 4. Performance Analysis of Malicious Nodes

The energy consumption analysis is performed with existing methods and the outcomes of such measurement are projected in detail in table 4. The suggested RTNIDBMAF has created minimum energy consumption when compared to existing methods. The proposed RTNIDBMAF has produced 52%,56%,61% of energy utilization in the existence of 50 nodes,100 nodes and 200 nodes in the network which is minimum than Power Efficient Adaptive Clustering Method (PEACM), Decentralised Cluster Based Routing Method (DCBM)

techniques, Reliability Based Intrusion Detection Techniques (RBIDT), Multiple Judge Reward Method (MJRM).

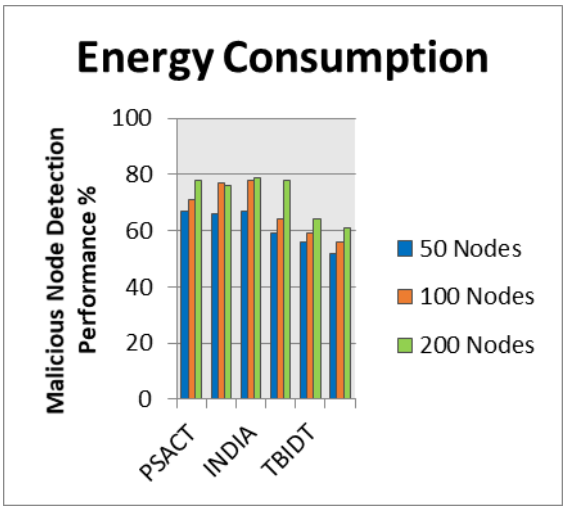

Fig. 6. Energy Consumption Analysis

The graph in fig.6. displays the efficiency in energy consumption analysis performed with comparing various existing methods such as PEACM, DCBM, RBIDT, MJRM.

5.1.4 Security Performances:

The security efficiency of the system is determined in relation to the quantity of threats identified for the total quantity of threats developed. The measurements are as follows:

$$\text{Security Performance} = \frac{Number\ of\ Threats\ Detected}{Total\ Number\ of\ Threats\ generated}$$

Security Performance Analysis			
	50 Nodes	100 Nodes	200 Nodes
PEACM	65	68	71
DCBM	67	71	74
RBIDT	71	74	77
MJRM	75	79	83
RTNIDBMAF	86	92	97

Table 5. Security Performance Analysis

The security performance is analysed with existing methods and the outcomes of such measurement is projected in detail in table. The suggested RTNIDBMAF has created maximum security performance when comparing to existing methods. The proposed RTNIDBMAF has produced 86%,92%,97% of security performance in the existence of 50 nodes,100 nodes and 200 nodes in the network which is greater than Power Efficient Adaptive Clustering Method (PEACM), Decentralised Cluster Based Routing Method (DCBM) techniques, Reliability Based Intrusion Detection Techniques (RBIDT), Multiple Judge Reward Method (MJRM).Fig 7. displays the security performance of the developed RTNIDBMAF method is evaluated with various existing methods such as PEACM, DCBM, RBIDT, MJRM.

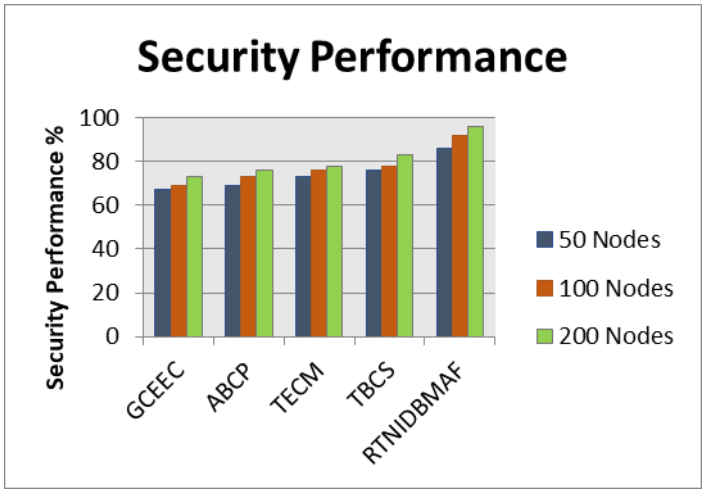

Fig.7. Security Performance

6. Conclusion

The reliability and energy consumption are significant key points of designing a network. Still, it is a difficult process to model the various functions in Mobile Ad-hoc Networks (MANET) due to its compact size, minimum bandwidth, less energy and memory. A secure and energy effective method is developed to increase the network stability when transferring the data from source node to destination node. In calculating the trust value of each node, the most optimal cluster Header (CH) node is chosen in the first stage. These reliability values are being compared to the threshold value and are the actual values. If the value is less than the referred threshold values, it confirms that a malicious node has entered the networks which can be eliminated by a malicious node detection and removal algorithm. Finally, the proposed method uses the public key cryptographic algorithm for providing the optimized and secure routing in Mobile Ad-hoc Networks (MANET). The proposed algorithm framework improves the Quality of Services (QoS) during the data transmissions in routing.

Acknowledgements

We thank our colleagues from SRM Institute of Science and Technology who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper..

Author contributions

S.Gnanavel: Conceptualization, Methodology, Software, Field study. **S. Muruganandam:** Data curation, Writing-

Original draft preparation. **G.Balamurugan:** Visualization, Investigation, Writing-Reviewing and Editing. **N.Duraimurugan:** Software, Validation, Field study

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Shobitha, G.S., Prabhakar, B. &Ghivela, G.C. Energy aware African buffalo-based optimized dynamic media access control protocol for mobile Adhoc network environment. Int. j. inf. tecnol. (2023). https://doi.org/10.1007/s41870-023-01372-x.

[2] Abdulai, JD., Adu-Manu, K.S., Katsriku, F.A. et al. A modified distance-based energy-aware(mDBEA) routing protocol in wireless sensor networks (WSNs). J Ambient Intell Human Comput 14, 10195–10217 (2023). https://doi.org/10.1007/s12652-021-03683-y.

[3] Mischos, S., Dalagdi, E. & Vrakas, D. Intelligent energy management systems: a review. ArtifIntell Rev 56, 11635–11674 (2023). https://doi.org/10.1007/s10462-023-10441-3.

[4] R. Ramesh and G. Seshikala, "Link Aware Multipath Routing to Defend Against Black Hole Attacks for MANETs," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-6, doi: 10.1109/CONIT59222.2023.10205694.

[5] S. Muruganandam, J. A. Renjit and R. S. Kumar, "A Survey: Comparative study of security methods and trust manage solutions in MANET," 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2019, pp. 125-131, doi: 10.1109/ICONSTEM.2019.8918697.

[6] Singh, C.E., Singh, J.A.P. (2023). An Investigation of Machine Learning-Based IDS for Green Smart Transportation in MANET. In: Agarwal, P., Khanna, K., Elngar, A.A., Obaid, A.J., Polkowski, Z. (eds) Artificial Intelligence for Smart Healthcare. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-23602-0_5.

[7] W. Bouassaba, A. Nabou and M. Ouzzif, "Review on Machine Learning Based Intrusion Detection for MANET Security," 2022 9th International Conference on Wireless Networks and Mobile Communications (WINCOM), Rabat, Morocco, 2022, pp. 1-6, doi: 10.1109/WINCOM55661.2022.9966457.

[8] A. Boyaci, H. H. Balik and F. Ata, "Energy-Aware Routing Architecture for Wireless Sensor Networks," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800791.

[9] Yu, Y., Liu, Y., Wong, D., Tang, SK. (2024). Comprehensive Performance Evaluation of Mobile Networks in Macao Based on Field Test Data. In: Yang, XS., Sherratt, R.S., Dey, N., Joshi, A. (eds) Proceedings of Eighth International Congress on Information and Communication Technology. ICICT 2023. Lecture Notes in Networks and Systems, vol 695. Springer, Singapore. https://doi.org/10.1007/978-981-99-3043-2_14

[10] Muruganandam, S., ArokiaRenjit, J. (2022). A Node Quality Based Cluster Header Selection Algorithm for Improving Security in MANET. In: Shetty, N.R., Patnaik, L.M., Nagaraj, H.C., Hamsavath, P.N., Nalini, N. (eds) Emerging Research in Computing, Information, Communication and Applications. Lecture Notes in Electrical Engineering, vol 789. Springer, Singapore. https://doi.org/10.1007/978-981-16-1338-8_11

[11] Muruganandam, S., Renjit, J.A. Real-time reliable clustering and secure transmission scheme for QoS development in MANET. Peer-to- Peer Netw. Appl. 14, 3502–3517 (2021). https://doi.org/10.1007/s12083-021-01175-6.

[12] Saravanan R., Swaminathan A., Balaji S. An intelligent shell game optimization based energy consumption analytics model for smart metering data. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2023, vol. 23, no. 2, pp. 374–381. doi: 10.17586/2226-1494-2023-23-2-374-381

[13] Tatarnikova T.M., Bimbetov F., Gorina E.V. Algorithm for energy-efficient interaction of wireless sensor network nodes. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2022, vol. 22, no. 2, pp. 294–301 (in Russian). doi: 10.17586/2226-1494-2022-22-2-294-301

[14] L. Legashev and L. Grishina, "Development of an Intrusion Detection System Prototype in Mobile Ad Hoc Networks Based on Machine Learning Methods," 2022 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation, 2022, pp. 171-175, doi: 10.1109/RusAutoCon54946.2022.9896238.

[15] D. Anuradha, R. Srinivasan,T. Ch. Anil Kumar,J.FarithaBanu,Aditya Kumar Singh Pundir and D. VijendraBabu"Energy Aware Seagull Optimization-Based Unequal Clustering Technique in WSN Communication,Intelligent Automation & Soft

Computing,IASC, 2022, vol.32, no.3,Page No:1326-1341,DOI:10.32604/iasc.2022.021946.

[16] RajarajeswariPerepi, Santhi K, Pratik Chattopadhyay & Anwar Bég O(2022): A deep learning computational approach for the classification of COVID-19 virus,Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, DOI: 10.1080/21681163.2022.2111722

[17] Pandey, P., Singh, R. QoS based modified route discovery in MANET for multimedia applications. Multimed Tools Appl 82, 29671–29688 (2023). https://doi.org/10.1007/s11042-023-14855-7

[18] Meena Pundir,Jasminder Kaur Sandhu,PuneetKumar,PrateekSrivastava,Secure and Energy Efficient Routing in Wireless Sensor Network using Machine Learning,ACM Digital Library,IC3-2022: Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing August 2022 Pages544–549,https://doi.org/10.1145/3549206.3549299

[19] Divyansh Puri and Bharat Bhushan. 2019. Enhancement of security and energy efficiency in WSNs: Machine Learning to the rescue. Proceedings - 2019 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2019 2019-January:120–125. https://doi.org/10.1109/ICCCIS48478.2019.8974465

[20] Muruganandam, S. ., Srinivasan, N. ., & Sivaprakasam, A. . (2022). An Intelligent Method for Intrusion Detection and Prevention in Mobile AdHoc Networks. International Journal of Intelligent Systems and Applications in Engineering, 10(3), 154–160. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2151

[21] G. Balamurugan and K. Kishore Anthuvan Sahayaraj, "A Blockchain Based Certificate Authentication System," *2023 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICCCI56745.2023.10128289.

[22] Balamurugan, G., Jayabharathy, J. (2022). A Comparative Analysis of Event Detection and Video Summarization. In: Hu, YC., Tiwari, S., Trivedi, M.C., Mishra, K.K. (eds) Ambient Communications and Computer Systems. Lecture Notes in Networks and Systems, vol 356. Springer, Singapore. https://doi.org/10.1007/978-981-16-7952-0_54

[23] Balamurugan G, Jayabharathy J. An integrated framework for abnormal event detection and video summarization using deep learning. International Journal of Advanced Technology and Engineering Exploration. 2022; 9(95):1494-1507. DOI:10.19101/IJATEE.2021.875854.

[24] G. Balamurugan and J. Jayabharathy, "Abnormal Event Detection using Additive Summarization Model for Intelligent Transportation Systems" International Journal of Advanced Computer Science and Applications(IJACSA),13(5),2022, http://dx.doi.org/10.14569/IJACSA.2022.0130586

[25] G. Balamurugan and V. Premanand, "A novel framework for extraction of landscape areas and automatic building detection in satellite images," *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014575.

[26] Francesco Cauteruccio, Giancarlo Fortino, Antonio Guerrieri, Antonio Liotta, Decebal Constantin Mocanu, Cristian Perra, Giorgio Terracina, and Maria Torres Vega. 2019. Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance. Information Fusion 52: 13–30. https://doi.org/10.1016/J.INFFUS.2018.11.010

[27] MohammadWazid and Ashok Kumar Das. 2016. An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks. Wireless Personal Communications 2016 90:4 90, 4: 1971–2000. https://doi.org/10.1007/S11277-016-3433-3

[28] Shanmugam, S. P. ., Vadivu, M. S. ., Anitha, D., Varun, M., & Saranya, N. N. . (2023). A Internet of Things Improvng Deep Neural Network Based Particle Swarm Optimization Computation Prediction Approach for Healthcare System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 92–99. https://doi.org/10.17762/ijritcc.v11i4s.6311

[29] Dhabliya, D. (2021). Feature Selection Intrusion Detection System for The Attack Classification with Data Summarization. Machine Learning Applications in Engineering Education and Management, 1(1), 20–25. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/8