Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 7297208, 10 pages
https://doi.org/10.1155/2023/7297208

Research Article

Relay Node-Based Routing Algorithm for Reducing Latency in Industrial Mobile Communication Network

Hatem S. A. Hamatta,[1] **Abdul Basit**,[2] **K. A. Sharada**,[3] **Y. Venkateswara Reddy**,[4] **K. Ragavan**,[5] **Mohiuddin Ali Khan**,[6] **Arvind Kumar Shukla**,[7] **Vivek Singh Kushwah**,[8] **and Roviel Berhane**[9]

[1]*Department of Applied Sciences, Aqaba University College, Al Balqa Applied University, Aqaba, Jordan*
[2]*Department of Computer science and Information Technology, Maulana Azad National Urdu University, Hyderabad, Telangana, India*
[3]*Department of CSE, HKBK College of Engineering, Bangalore, Karnataka, India*
[4]*Department of Electronics and Communication Engineering, Malla Reddy Institute of Technology, Hyderabad, India*
[5]*Department of ECE, Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India*
[6]*Department of Computer and Network Engineering, Jazan University, Jazan, Saudi Arabia*
[7]*Department of Computer Applications, IFTM University, Moradabad, Uttar Pradesh, India*
[8]*Department of Electronics and Communication Engineering, Amity School of Engineering and Technology (ASET), Amity University Madhya Pradesh, Maharajpura Dang, Gwalior, India*
[9]*Department of Chemical Engineering College of Biological and Chemical Engineering, Addis Ababa Science and Technology University, Addis Ababa, Ethiopia*

Correspondence should be addressed to Hatem S. A. Hamatta; hatem@bau.edu.jo
and Roviel Berhane; roviel.berhane@aastustudent.edu.et

Received 16 May 2022; Revised 19 July 2022; Accepted 15 April 2023; Published 20 June 2023

Academic Editor: Kalidoss Rajakani

Mobile network nodes perform time transfer during data packet performance in an asynchronous manner. Network nodes get packets for transmission from node sensors that reject the demands of node attackers. When packet loss occurs unexpectedly due to a network removal, it is exceedingly difficult to detect assaults and time forwarding. Attack detection accuracy deteriorates, and packet loss rates rise. A strategy for node mobile intermediate that gets over attacks that identify the forward choosing is provided for improved data forwarding. Network performance is completely damaged by specific attacks, such as communication processes that degrade or lose packets. The algorithm's architecture ensures that the best nodes are chosen for relaying and that transmission packets that do not drop are declined. To enable the node and create an effective path routing, a process is executed. Decreasing the amount of packet loss and increasing attack efficiency are being identified.

1. Introduction

The mobile network accepts the user in its environment such as the performance of the protected monitor network, irregular behaviour to evade the worry protection, and lack of middle coherence in the middle. As a result, distinct layers of intruders may alter in a mobile environment. In a mobile network, there are many layers for available intrusions [1]. While nodes are malfunctioning due to intrusions at the layer linking the data, denial of communication is misbehaving at the application layer. Intruders use a variety of techniques, such as dropping poles, withholding connections, black holes, spoofing connections, and Sybil, to determine where they are in the network and how to get in [2].

When an intruder drops data, the mobile environment network is under attack. When an intrusion packet was dropped, nodes that were relaying traffic were identified in order to focus on abnormal nodes [3]. As a result, communication is via terminal means intruder, and the entire piece of information is lost [4]. Node specification from packet data is the broadcast node sender. A node that should be malicious from the packet loss technique is created by the mobile environmental network problem. They argue that the count sequence objective is larger to contain the intruder issue performance [5]. According to node intruder resources, with a higher load, communication should be disrupted because of resource overload, which causes packet traffic to transmit from the initiate's node sender. The issue of malicious behaviour that could reject the selected issue of an invader grey hole or target network-specific packet data, that is, the part picked at random, was removed from all packet sharing [6]. To prevent various intruders from being identified by lost packets, intruders for a group could be considered an intruder's characteristic [7].

To break the oath that is used and contains independent loops, a multiple data routing strategy is available. The method is to employ the reliable communication route that provides an intrusion loss packet [8]. According to the means record, the ambient mobile network, which was the layer of the network layer known to identify the intrusion that caused a packet loss attack, was avoided. The drop packets were used to avoid opportunities from node intruders with paths that were fully recognised by the node network during the communication period [9].

Regular topological network changes could cause the best possible routing path to become ineffective immediately [10]. The strong network should be designed with a built-in mobile routing network. Even though the environmental network was based on information for global requirements, there is no middle structure in the network because there are no adjacent operations that can be included in this design [11]. As we have already indicated, the needs of distinct groups merged with the way the nodes functioned. It is simple to control the node entity through packet organisation with a maximum range that classified the complete ant colony. To fully realise one's potential, nodes of resources were present throughout the entire communication process [12].

The remaining sections of the paper are as follows. Section 2 provided related works. Section 3 provides enhanced improved data forwarding scheme that contains information about a method that assists in node target from the sender in which concentrates the attack on specific forwarding nodes. Section 4 mentioned simulations of performance analysis and result analysis with various parameters. The research's conclusion and the research's future work are discussed in Section 5.

2. Related Work

Node terminals developed by Wu et al. [13] were based on social network characteristics that specifically take into account mobile social network delay tolerance. Assume that the mobile ad hoc protocol routing is complete for node target and node source among the path communication. It adapted with amazing skill to the way that logical dynamic MSN were dealt with using an optimization colony based on algorithm routing. The MSN trait of being a social network is present. Data forwarding and updating strategies were used in the ACOMSN methodological design.

According to Quang and Kim [14], the wireless sensor network in industries for information was improved with real-time performances of real-time gradient routing. The suggested algorithm for routing is based on the two-hop information, which is determined by the number of hops with a certain distance to the sink, and routing velocity of two-hop that has been adopted. Additionally, computing complexity and energy consumption result in a reduction in the scheme's control acknowledgment.

Zhang et al. [15] found a solution to the energy balancing issue, and WSNs are highly essential routing algorithms that ensure the quality of service while being energy-efficient. Data categories and defined priorities were used to categorise the industrial training. Consumption energy has the equilibrium that set node forwarding candidate that establishes and the purpose of effective communication cannot be with common data and timely reliable with sink node that sent data sensing was crucial in industries. When the data was high in exhibiting simulation results, the data kinds were more trustworthy in real-time transmission.

According to Chourasia and Boghey [16], many nodes were created as a group with the creation of the MANET. While interacting with all those who have minimal resources, the current node in MANET is malevolent, degrading the network performance in a dynamic way, and this affects routing performance. Continually hostile nodes cause the neighbouring response node to redirect all requests. The routing method, which is in charge of node intermediates, continues movement. Attacks against the security of the suggested method were made in the network node by malicious packet dropping. The information or data that linked the sender and the receiver together to discover an idea was done by an attacker who would then suggest a viable scheme. Receivers from the sender were not available with enough activity to spot a malicious node neighbor's intermediate. It reduces dropped and received data to enhance intended routing security in network data.

According to Sangaiah et al. [17], a boost in productivity and duty was focused on the work of supervising factories with a lot of activity. With node sensors' limited energy supply, these networks are essential to ensuring optimal energy utilisation. The goal of coverage and tracking is to consume energy efficiently. Sensors were notified by cluster head nodes, and their weights were calculated. The predefined weight has a maximum connection to the cluster head route that sends signals in the network.

According to Fang et al. [18], the WSN industries are based on computer fog and use unique wireless network sensors which provide reduced latency transfer of information, quick resource scheduling, and real-time control. Internal attacks present a significant security challenge for the network distribution. The typical security measures used in different attacks involve trade-offs between security and information convergence, which is necessary to fulfill energy consumption and transmission requirements. Energy consumption and performance transmission were balanced in order to introduce the concept of making grey decisions. Secure routing based on management confidence, reliable nodes, and the trade was suggested for effective selection.

According to Khudayer et al. [19], emergency operations and environmental protection are two areas where humans support MANET, which has set the way for swiftly advancing wireless industrial communication. The topology of the network changes as a result of a MANET source routing problem, and the discovery of request routing increases the frequency of broken links. Researchers suggested ZRDM and LFPM as two techniques for source routing that improve on-demand. In order to avoid the route that is intended for LFPM, node mobility that generates breakage forces the route request flooding to aim for ZRDM. Performances of the processes for which we suggested the experiment, such as the dynamic source routing protocol, are well known.

According to Luo et al. [20], the routing protocol which is based on WSN concerns a significant portion of energy-saving optimization; the availability of sensor nodes with the most factual battery power is limited. Network queue relay one-dimensional data that minimises energy usage and maximises network lifetime. To enable the most energy-saving opportunistic routing, energy residual must be minimal in comparison to the node's cost and power.

3. Overview of the Proposed Scheme

The unsequenced node of mobile has the period of communication as its intrinsic property. The network environment in the node receives the packet data from the node sender in order to reject the node attacker's intention. The packet data that transmits node instance for each time is of higher quality than the packet data that are lost. Environmental network mobile cannot easily handle the intruder kind, as the node among the communication that initiates while packet data drops erratically. When using this technique, the rate of packet drop and the effectiveness of attacks were decreased.

The method we suggested in this paper, known as enhanced improved data forwarding, is employed for environmental node relaying to the forward selective through categorization. Intruders may refuse the transmission of packets in the node operation when a network characteristic is completely damaged, such as when a packet is dropped. As long as there will be no packet data loss and communication is not refused, the built-in enhanced efficient relaying node algorithm selections were permitted. The efficient routing path was designed, and packet transmission was carried out to authorise the node. Rate drop packets were reduced, and the efficiency of the detection was improved.

The suggested enhanced improved data forwarding method is shown in Figure 1. Every data had to be measured by the range for the transmission packet node, and the packet transmission time was limited to packets that could be received or sent with a particular quantity. Selective forwarding in a network environment in which node destinations were sent to node sources for packet sharing is refused in advance with node attacker. The standard and intruder forwarding selection that categorise the employed method of enhanced improved data forwarding were presented in the environmental network in relaying node. The enhanced effective relaying node selection algorithm's optimal node is selected for the routing. The efficiency of detection has increased while the rate of packet drops has decreased.

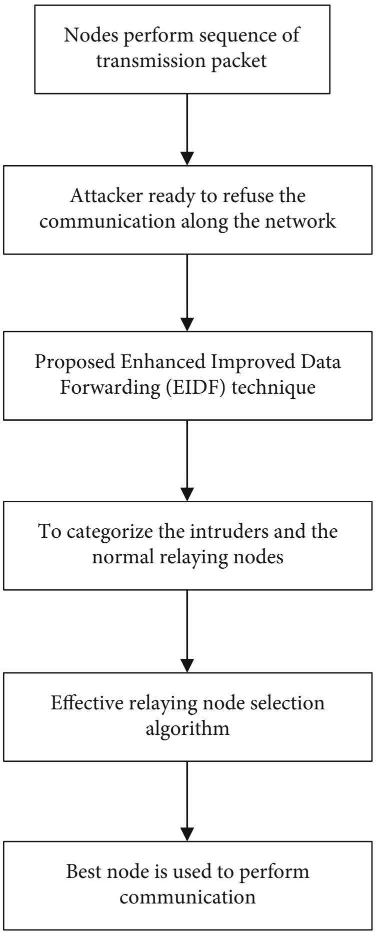

Nodes perform sequence of transmission packet
Attacker ready to refuse the communication along the network
Proposed Enhanced Improved Data Forwarding (EIDF) technique
To categorize the intruders and the normal relaying nodes
Effective relaying node selection algorithm
Best node is used to perform communication

Figure 1: The proposed enhanced improved data forwarding (EIDF) technique.

3.1. Sequence of Packet Transmission by Node. In order to fulfill a request for a packet specification, the node sender has to accept several reply packets during the routing process. The node targets that accepted the packet request and the number of sequence are the initial conditions for the path's method for verification. Table routing is kept at its highest value, along with the access path that determines which node should receive the destination node for a packet request that was just sent. The following circumstance is to hop that the node target is the range similar to the count sequence of residue. The value of the hop count, which is preserved in the table routing as a substitute for node targets, is then used to determine how recently transmitted packet replies should be accessed. Hops were of low quality of node with route choices, end-to-end distance is equal, so the path efficient is picked to count the minimum value for protocol routing to appear. Due to the dynamic movable topology of the network, the quality of hops was prioritized as the option with the lowest likelihood of achieving the desired end distance for similar nodes via newly created links and recently assembled nodes.

$$\mathrm{SC} = \mathrm{EP} + \mathrm{IDC}, \tag{1}$$

where SC is the sequence communication. EP is the effective path. IDC is the improved data forwarding.

Optional paths included options for surveying and node hopping with shorter end-to-end distances under identical conditions with other conditions being permitted. There are two different conditions after it. Node target stated that the path routing effectively chooses protocol routing measure. The main problems with protocol routing are the network in node relaying, stored access route relaying, condition modification, path node relaying, and route invalidation. While an access path is doing so, routers invalidate access and build nodes that should be relaying each packet, accepting packet requests, and accepting packet replies.

$$\mathrm{IDF} = \mathrm{PF} \times \mathrm{AD}, \tag{2}$$

where PF is the packet flow. AD is the attack detection.

In order to build that node, the packet request that accepts node relaying should circle the table in order to access the route backward. An individual route for moving the nodes that makes up the arrow. Node target is on the road that leads to discovering a packet request for a different product from a node source that is comparable to the one that is being considered for us. The nodes with space velocity maximum towards the node relay that are travelled to the nearer, easier node. This is how the node hops similar quality with different routes throughout the packet request that access the node should relay similarly with it. Then, the node accepts the packet request, established the route to assume, and narrows. Requested packets come from achieved count sequence senders that distinguish which nodes should broadcast the protocol.

$$\begin{gathered} \mathrm{PF} = \mathrm{SRQ} + \mathrm{SRE}, \\ \mathrm{S}\left(\mathrm{RQRE}\right) = \mathrm{SRQ} + \mathrm{SRE}, \end{gathered} \tag{3}$$

where SRQ is the success of the request packet. SRE is the success of a replay packet.

The table routing maintained the details and packet requests for the value of the count node. They are similar to the count sequence, which is equal, and they are also similar to the range of the hop count and the routing table that does not modify the relaying node. It altered the path recently due to the weather, path routing has good intentions with it, and sharing packet data is to guide speed. In the network, the node sender in the direction with packet reply transmits and produced the node target that agreed while it occurs in the same condition. The details and packet request value of the count node are recorded in the table routing. The hop-count range and count sequence, as well as the routing table that does not change the relaying node, are likewise identical. The recently changed path is good with sharing packet data speed to the point. The network's node sender consented to broadcast packet replies in the direction of the created node target while the situation persisted.

3.2. Enhanced Improved Data Forwarding (EIDF) Technique. The nodes of the sender, the target, and the remaining nodes show the identical characteristic that should be among two nodes with path that is quickly available and packet data transmit to reach the considered node sender. The node's location is where the path starts in this scenario. The sender of the initial request is the transmit node. Node of quality is similar with the network in that it presents many routes. Despite the network in the node being close by and depending on the lowest route distance, the path is frequently chosen for protocol routing. The route is chosen to be lower, making the node easier to complete when doing packet transfer.

$$\mathrm{AD} = \mathrm{Discover} + \mathrm{Decline}. \tag{4}$$

The network, along with data sharing, is easier to lead than the upper path that should be selected consequently. The route is chosen based on the packet requests that convey the sender's requirements. The count series that differs from request path transmission is comparable to expect ID node broadcasting. Hop nodes of equivalent quality are previously selected using path routing and are continuing similar packet requests through loss with the routing protocol. Additionally, it determines the packet request that anticipates the next step, space minimization with path routing is needed to establish the need, and the route should be structured. To achieve the shortest amount of time, the relay node should follow the packet request when the routing is in the starting direction for node relay and effective path routing for packet requests that should be made earlier than the node targets. It is not taken into account by the protocol routing, and an effective route need not do a selection calculation. Utilizing the enhanced improved data method, the intruders were divided into groups. The assumptions included forwarding, node routing, and various conditions. Node packet sharing was quicker, which allows for better route selection.

$$\mathrm{AD} = \mathrm{Discover}\left(\mathrm{SDF}\right) + \mathrm{Decline}\left(\mathrm{SDF}\right). \tag{5}$$

Target node receives a packet reply from the packet reply node with a time stamp for the packet request and with unrestricted access next to the access table indicating that the target node has been maintained for routing. Packet requests with value estimations for the route's access render the insect that should be the relaying node invalid. If the sender node is similar to the target node that accepts the request, table access routing that kept significant that equivalent count node packet request and count series that is similar, then the packet requests the value of routing should monitor the node target and maintenance value of routing table. When a routing packet request is made, the routing table's value must be at a minimum. When a target node is reached, the routing table

```
Step 1: in the path different relay node analysis
Step 2: relay node which is chosen
Step 3: packet transmission with initial sequence
Step 4: trusted node is verified
Step 5: if {node == trust}
Step 6: communication allocation
Step 7: else
Step 8: if {node == Attacked}
Step 9: communication decline
Step 10: data packet loss
Step 11: for routing different node search
Step 12: end if
Step 13: end for
```

Algorithm 1: Algorithm for enhanced improved data forwarding (EIDF) technique.

```
Step 1: rate of forwarding data is monitored
Step 2: selection node is efficient for each one
Step 3: if {relaying node == efficient}
Step 4: node efficient was selected
Step 5: path is constructed
Step 6: else
Step 7: if {relaying node!= efficient}
Step 8: they do not choose the node efficient
Step 9: end if
Step 10: efficient detection increases, and the rate of loss reduces the packet
Step 11: end for
```

Algorithm 2: Algorithm for enhanced efficient relaying node selection.

should be updated, and a new reply packet message reply is sent.

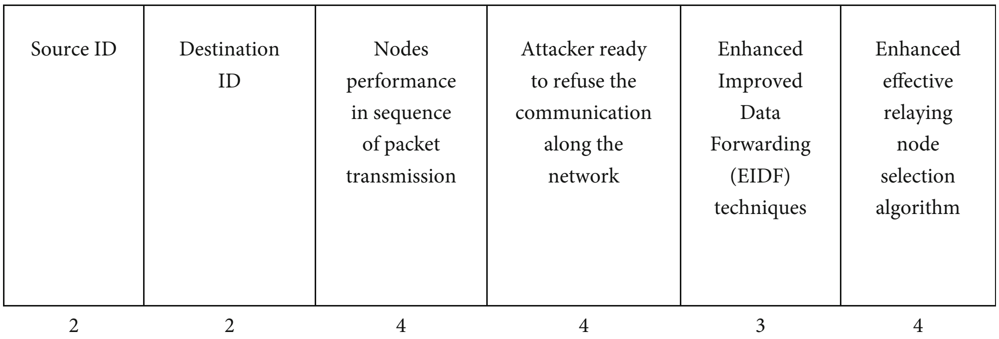
$$\begin{aligned} \mathrm{AD} &= \mathrm{SDF}\,(\mathrm{Discover} + \mathrm{Decline}), \\ \mathrm{IDF} &= \mathrm{S}(\mathrm{RQRE}) \times \mathrm{SDF}\,(\mathrm{Discover} + \mathrm{Decline}). \end{aligned} \tag{6}$$

Count series verification from the table path, count node forwarding data, count node attacker forwarding selective, and count packet reply or request that verifies the node relay. Value forwarding data is focused on the node relaying, and table routing is to preserve the value that counts series to equate the count of series. Value forwarding data is the least amount of data with a table based on the value forwarding data packet, rate forwarding data comparable to an access route backward, or an access route forwarding data modifier to the relaying node following. However, node target and node sender among the identified recent routes are equivalent to a packet replay or request. The maximum rate forwarding data table is similar, and the most recent packet requests that lose data typically go towards the target node. When a packet requests retransmission and a node is replaying it, the network's routing database does not establish that path access. The node quality and count series in table routing are comparable to the current route. Rate the least forwarding data with a packet reply that offers valuable forwarding data to confirm the node's answering. Data packet sharing is the method utilised in this, and the path was well-organized [21–34].

3.3. Enhanced Efficient Relaying Node Selection Algorithm. Node neighbour is the first and second hop to determine whether the network in which a node may operate and packet message is aware that is comparable to the time of location broadcast, according to the enhanced relaying node selection algorithm. Locations with packet message awareness that spread the technique flood in their purest form. Data packets are broadcast in a fashion that is so inefficient in floods and troughs; nonetheless, the transmission was well-organized, with more network traffic following the node-relaying selection stage. The procedure that additionally transmits the location awareness and distributes locations concurrently with sequence must begin with essential overflow with selection node relay commencing the process.

$$\begin{aligned} \mathrm{EP} &= \mathrm{Select}\,(\mathrm{RN}), \\ \mathrm{SC} &= \mathrm{Select}\,(\mathrm{RN}) + (\mathrm{S}(\mathrm{RQRE}) \times \mathrm{SDF}\,(\mathrm{Discover} + \mathrm{Decline})). \end{aligned} \tag{7}$$

Upon accepting a specific transmit packet awareness, the position of the broadcast was previously with the weather and on the focused node source that we observed. Data packets are retransmitted with the node in order to list single



Source ID	Destination ID	Nodes performance in sequence of packet transmission	Attacker ready to refuse the communication along the network	Enhanced Improved Data Forwarding (EIDF) techniques	Enhanced effective relaying node selection algorithm
2	2	4	4	3	4

Figure 2: Proposed IDF packet format.

hop packet awareness locations of location node sources that we added with each node, as well as to determine whether one count with hop packet awareness locations of source node addresses that add with each node. With a dual list and a two-hop count, packet awareness locates addresses of node sources that are added with other nodes which accept packets. With the sender node, a single hop was not previously planned. The sum for the record of the source node's two hops includes the data packets that were shared with their single node's neighbour but should have been shared with the single node itself. During the communication period, packet data will not be dropped thanks to the routing's efficient node relaying.

Path routing in communication nodes relaying allows for the building of an improved efficient node selection technique. Due to the attacker's ability to forward the avoid option, there was a significant loss of data packets during the conversation interval. Minimum packet drop rate and effective detection are improved.

3.3.1. Packet ID. Information about the mobile node contains each packet ID. The table of every node in the routing is stored, and the performances of mobile node are communicable, as we observed.

Figure 2 depicts the enhanced improved data forwarding (EIDF) method that we suggested and illustrated to format the packets. Each field of the ID node's destination and source carried 2 bytes. The transmission packet carrying the third performance node's sequence was 4 bytes long. Four bytes were taken from the fourth one's field. The network along with communication was equipped to prevent attackers, and the communication along with packet transfer prevents the attack with selective data forwarding. Three bytes were occupied in the fifth place, and the enhanced imposed data forwarding (EIDF) technique, route communication, offers the free attack. In the last field, four bytes were taken with the algorithm of enhanced efficiency relying on node selection.

4. Performance Evaluation

4.1. Simulation Model and Parameters. Network simulator tool (NS 2.34) with simulated scheme enhanced improved data forwarding (EIDF). Simulation is based on a simulation time of 40 milliseconds for the region of 1160 meter × 920 meter square which has been placed with mobile ad hoc nodes 100. Network at various speeds among random manner with the mobile node. During this time, communication overloads the packet with a constant speed that provides constrain bit rate (CBR). Path routing is a free attack selectively obtained using the protocol demand on distance vector routing. Table 1 represents the estimation of the simulation setup.

Table 1: Simulation setup.

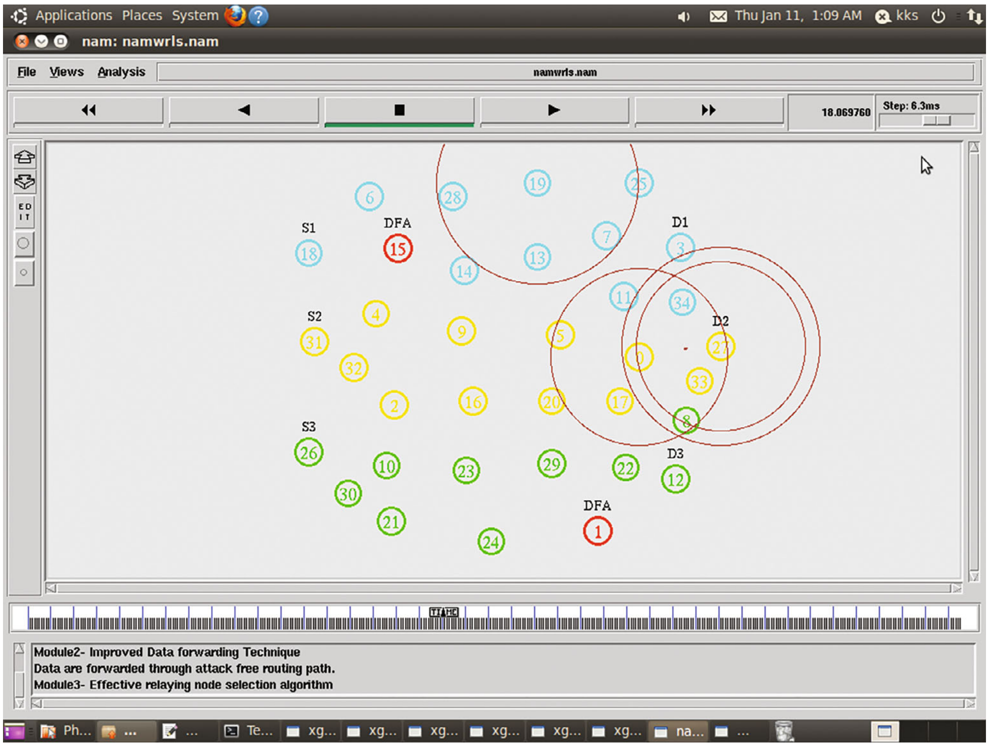
No. of nodes	100
Area size	1160 × 920
Mac	802.11 g
Radio range	250 m
Simulation time	40 ms
Traffic source	CBR
Packet size	512 bytes
Mobile model	Random waypoint
Protocol	AODV

4.1.1. Simulation Result. Figure 3 represents the scheme proposed for enhanced improved data forwarding (EIDF). It is compared with the attack forwarding data section to remove and detect the use of methods that exist in RA [13] and NIDS [16].

Node destination from the source node was a path-free routing to attack which provided the emission of attack that was used for the identification of EIDF in it. Node source from the packet reply has been provided as a free node of attack. The node behavior is observed to construct the algorithm of enhanced effective relaying node selection and node best selection. Rate of packet drop is minimized and efficient detection is increased.

4.2. Performance Analysis. In NS 2.34, graph X is used as performance metrics that follow the analysis of the simulation.

4.2.1. Energy Consumption. Figure 4 represents the consumption of energy, communication spend energy extension, and level of energy started and ended with consumption of energy calculation in that mean. Path routing is a free attack selective



Module2- Improved Data forwarding Technique
Data are forwarded through attack free routing path.
Module3- Effective relaying node selection algorithm

Figure 3: Proposed EIDF results.

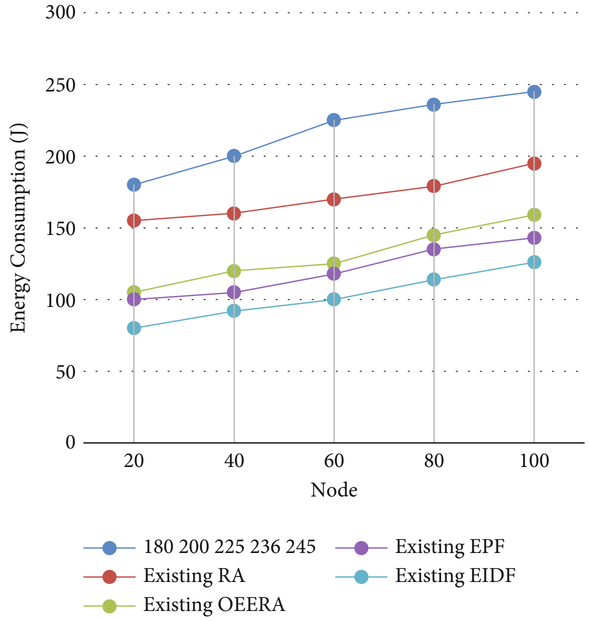


Figure 4: Nodes vs. energy consumption.

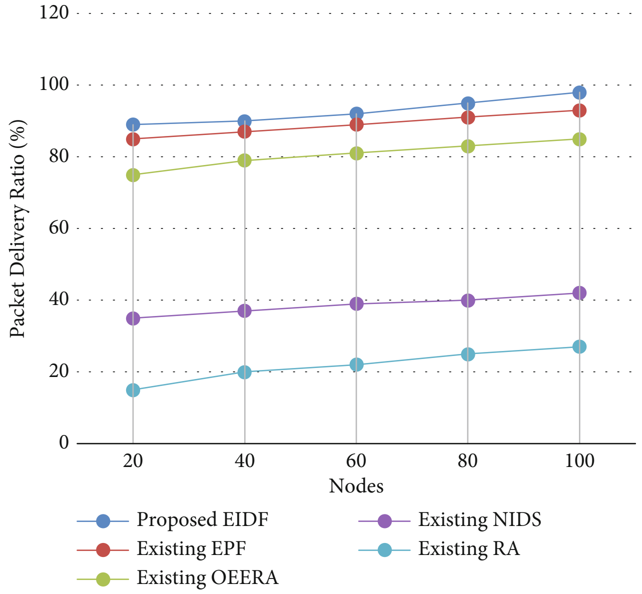


Figure 5: Nodes vs. packet delivery ratio.

that provides with the method of proposed enhanced imposed data formatting (EIMF). The existing method has been compared to reduce the consumption of energy with EPF, NIDS, OEERA, and RA.

$$\text{Energy consumption} = \text{Initial energy} - \text{Final energy}. \qquad (8)$$

4.2.2. Packet Delivery Ratio. Figure 5 represents the speed particular which has sent number of packet-to-number of received, the measured ratio of packet delivery. At 100 bps, the mobility is fixed with simulation, which is not constant with the velocity node. The existing method that has been compared to improve the ratio of packet delivery with EPF, NIDS, OEERA, and RA.

$$\text{Packet delivery ratio} = \left(\frac{\text{Number of packet received}}{\text{Sent}}\right) \times \text{Speed}. \qquad (9)$$

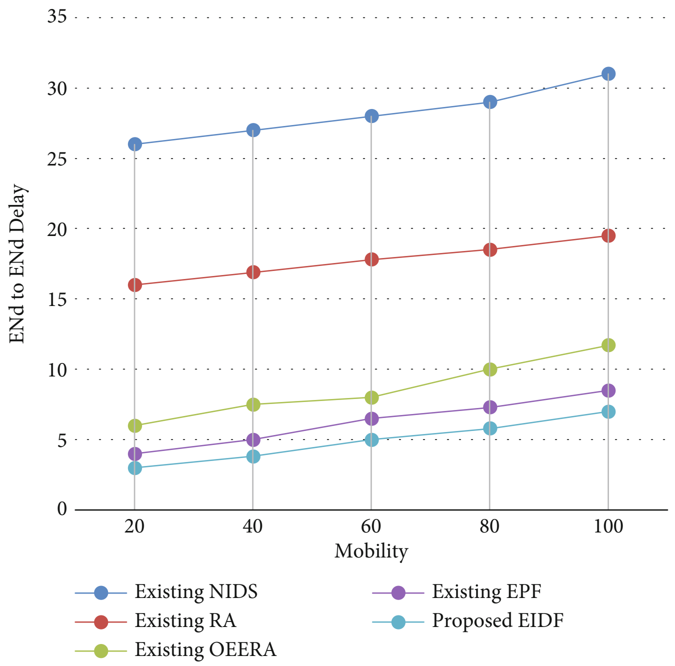


Figure 6: Mobility vs. end-to-end delay.

4.2.3. End-to-End Delay. Figure 6 represents the amount of time that estimated delay end to end used for node destination from node source in the transmission packet. Path routing normally provides a character node that traces from the designed algorithm of node proclivity tracing. The existing method has been compared to reduce the delay end to end with EPF, NIDS, OEERA, and RA.

$$\text{End to end delay} = \text{End time} - \text{Start time}. \quad (10)$$

4.2.4. Network Lifetime. Figure 7, represented by the node process, is measured with network lifetime. The ability of the network, overall, from network utilization that is taken and routing for node effectiveness has been chosen to construct an algorithm enhanced efficient relaying node selection algorithm. The existing method has been compared to increase the network lifetime with EPF, NIDS, OEERA, and RA.

$$\text{Network lifetime} = \frac{\text{Time taken to utilize network}}{\text{Overall ability}}. \quad (11)$$

4.2.5. Packet Drop Rate. Figure 8 represents drop nodes from planned in the network that transmits all data that drop the packet because overload packet data, so technique enhanced improved data forwarding and path routing are good. The existing method has been compared to minimize the rate packet drop with EPF, NIDS, OEERA, and RA.

$$\text{Packed drop rate} = \left(\frac{\text{Number of packet losses}}{\text{received}} \times 100\right). \quad (12)$$

4.2.6. Detection Efficiency. Figure 9 represents the efficiency of detection, from node destination to node source to repeated transmission packet attack. In the scheme enhanced improved data forwarding, path routing is present, and attack selectively removes and identifies which has been used. The existing method has been compared to improved efficiency detection with EPF, NIDS, OEERA, and RA.

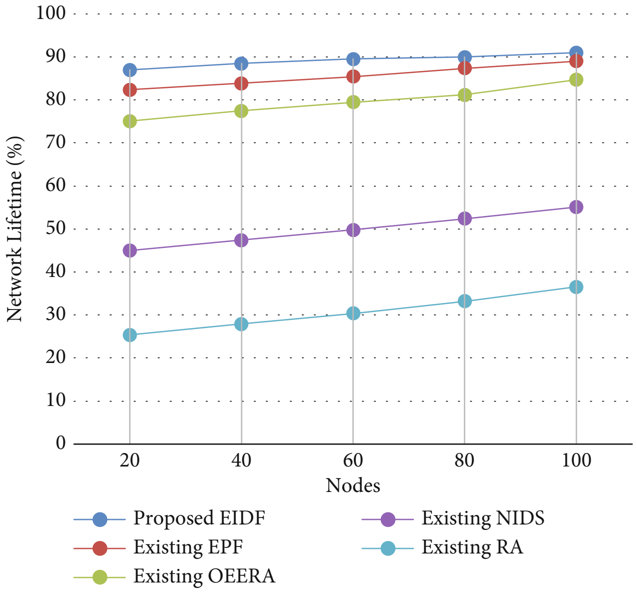


Figure 7: Nodes vs. network lifetime.

$$\text{Detection efficiency} = \frac{\text{Attack detection rate}}{\text{Overall time}}. \quad (13)$$

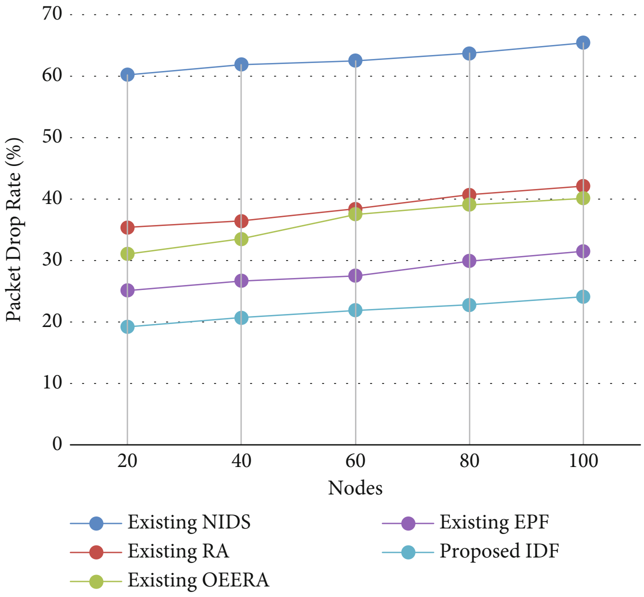


Figure 8: Nodes vs. packet drop rate.

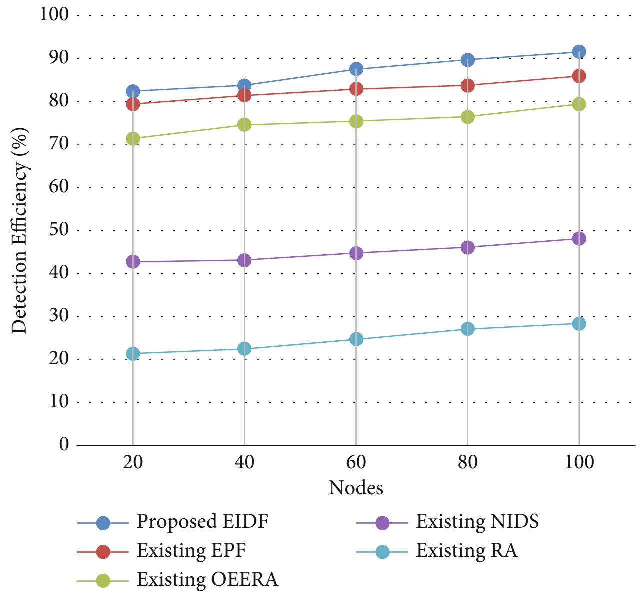


Figure 9: Nodes vs. detection efficiency.

5. Conclusion

The mobile node acts as an intermediary in the mobile network by communicating and rejecting node intrusions. The malicious node operations cause packets to be sent with higher-quality data loss. It was difficult to reject and identify the detrimental communication which should be spread farther with maximum packet loss rate and minimised attack detection efficiency. The approach suggested that enhanced improved data forwarding protects against intrusions that previously discovered the selective forwarding on mobile nodes. In order to hurt invaders, a routing network that reduces or drops packet sharing is necessary. To offer a hint to the constructed scheme that is effective, enhanced relay node that is efficient does not lose packets and rejects the process. Construction route is effective, and communication is a procedure that is performed to carry out the node's authorization. Rate packet loss is reduced, and detection attack efficiency is raised. The work focused on various parameter analyses of the MIMO-based fuzzy approach.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] T. Braun, M. Heissenbüttel, and T. Roth, "Performance of the beaconless routing protocol in realistic scenarios," *Ad Hoc Network*, vol. 8, no. 1, pp. 96–107, 2010.

[2] T. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, RWS Publications, 2001.

[3] Z. Wang, C. Li, and Y. Chen, "Local cooperative relay for opportunistic data forwarding in mobile ad-hoc networks," in *2012 IEEE International Conference on Communications (ICC)*, pp. 5381–5386, Ottawa, ON, Canada, 2012.

[4] A. Darehshoorzadeh and L. Cerd'a-Alabern, "Candidate selection algorithms in opportunistic routing," in *Proceedings of the 5th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, pp. 48–54, Bodrum, Turkey, 2010.

[5] M. Musolesi and C. Mascolo, "Car: context-aware adaptive routing for delay-tolerant mobile networks," *Mobile Computing, IEEE Transactions*, vol. 8, no. 2, pp. 246–260, 2009.

[6] B. Karp and H. T. Kung, "Gpsr: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 243–254, Boston, Massachusetts, USA, 2000.

[7] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *2013 UKSim 15th International Conference on Computer Modelling and Simulation*, pp. 693–698, Cambridge, UK, 2013.

[8] P. M. Jawandhiya, M. M. Ghonge, M. S. Dr, P. Ali, and J. S. Deshpande, "A survey of mobile ad hoc network attacks," *International Journal of Engineering Science and Technology*, vol. 2, no. 9, pp. 4063–4407, 2010.

[9] S. Vhora, R. Patel, and N. Patel, "Rank base data routing (RBDR) scheme using AOMDV: a proposed scheme for packet drop attack detection and prevention in MANET," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–5, Coimbatore, India, 2015.

[10] T. Shu and M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813–828, 2015.

[11] R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver, "A secure protocol for spontaneous wireless ad hoc networks creation,"

IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 4, pp. 629–641, 2013.

[12] S. Singha and A. Das, "Detection and elimination of the topological threats in mobile ad hoc network: a new approach," in *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 907–911, Ghaziabad, India, 2015.

[13] Y. Wu, Y. Zhu, and Z. Yang, "Routing algorithm based on ant colony optimization for mobile social network," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 297–302, Kanazawa, Japan, 2017.

[14] P. T. A. Quang and D. S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 1, pp. 61–68, 2012.

[15] W. Zhang, Y. Liu, G. Han, Y. Feng, and Y. Zhao, "An energy efficient and QoS aware routing algorithm based on data classification for industrial wireless sensor networks," *IEEE Access*, vol. 6, pp. 46495–46504, 2018.

[16] R. Chourasia and R. K. Boghey, "Novel IDS security against attacker routing misbehavior of packet dropping in MANET," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, pp. 456–460, Noida, India, 2017.

[17] A. K. Sangaiah, A. S. Rostami, A. A. R. Hosseinabadi et al., "Energy-aware geographic routing for real-time workforce monitoring in industrial informatics," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9753–9762, 2021.

[18] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, vol. 26, no. 5, pp. 3169–3182, 2020.

[19] B. H. Khudayer, M. Anbar, S. M. Hanshi, and T. C. Wan, "Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks," *IEEE Access*, vol. 8, pp. 24019–24032, 2020.

[20] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 112–121, 2015.

[21] C. R. Rathish and A. Rajaram, "Efficient path reassessment based on node probability in wireless sensor network," *International Journal of Control Theory and Applications*, vol. 34, no. 2016, pp. 817–832, 2016.

[22] S. Rahamat Basha, C. Sharma, A. N. Farrukh Sayeed et al., "Implementation of reliability antecedent forwarding technique using straddling path recovery in MANET," *Wireless Communications & Mobile Computing (Online)*, vol. 2022, article 6489185, pp. 1–9, 2022.

[23] C. R. Rathish and A. Rajaram, "Hierarchical load balanced routing protocol for wireless sensor networks," *International Journal of Applied Engineering Research*, vol. 10, no. 7, pp. 16521–16534, 2015.

[24] D. N. V. S. L. S. Indira, R. K. Ganiya, P. Ashok Babu et al., "Improved artificial neural network with state order dataset estimation for brain cancer cell diagnosis," *BioMed Research International*, vol. 2022, Article ID 7799812, 10 pages, 2022.

[25] P. Ganesh, G. B. S. R. Naidu, R. Korla Swaroopa et al., "Implementation of hidden node detection scheme for self-organization of data packet," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 1332373, 2022.

[26] A. Rajaram and K. Sathiyaraj, "An improved optimization technique for energy harvesting system with grid connected power for green house management," *Journal of Electrical Engineering & Technology*, vol. 2022, article 7799812, pp. 1–13, 2022.

[27] M. Dinesh, C. Arvind, S. S. S. Mole et al., "An energy efficient architecture for furnace monitor and control in foundry based on industry 4.0 using IoT," *Scientific Programming*, vol. 2022, Article ID 1128717, 8 pages, 2022.

[28] S. Kannan and A. Rajaram, "Enhanced stable path routing approach for improving packet delivery in MANET," *Journal of Computational and Theoretical Nanoscience*, vol. 4, no. 9, pp. 4545–4552, 2017.

[29] R. P. Prem Anand and A. Rajaram, "Effective timer count scheduling with spectator routing using stifle restriction algorithm in MANET," *IOP Conference Series: Materials Science and Engineering*, vol. 994, no. 1, article 012031, 2022.

[30] K. V. Kumar and A. Rajaram, "Energy efficient and node mobility based data replication algorithm for MANET," *International Journal of Computer Science*, vol. 2019, 2019.

[31] C. R. Rathish and A. Rajaram, "Sweeping inclusive connectivity based routing in wireless sensor networks," *ARPN Journal of Engineering and Applied Sciences*, vol. 3, no. 5, pp. 1752–1760, 2018.

[32] K. Mahalakshmi, K. Kousalya, H. Shekhar et al., "Public auditing scheme for integrity verification in distributed cloud storage system," *Scientific Programming*, vol. 2021, Article ID 8533995, 5 pages, 2021.

[33] J. Divakaran, S. Malipatil, T. Zaid et al., "Technical study on 5G using soft computing methods," *Scientific Programming*, vol. 2022, Article ID 1570604, 7 pages, 2022.

[34] S. Shitharth, P. Meshram, P. R. Kshirsagar, H. Manoharan, V. Tirth, and V. P. Sundramurthy, "Impact of big data analysis on nanosensors for applied sciences using neural networks," *Journal of Nanomaterials*, vol. 2021, Article ID 4927607, 9 pages, 2021.