Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.036916
Article

Improved QoS-Secure Routing in MANET Using Real-Time Regional ME Feature Approximation

Y. M. Mahaboob John[1,*] and G. Ravi[2]

[1]Mahendra College of Engineering, Salem, Tamilnadu, India
[2]Sona College of Technology, Salem, Tamilnadu, India
*Corresponding Author: Y. M. Mahaboob John. Email: mahaboobjohnmce@outlook.com
Received: 16 October 2022; Accepted: 08 December 2022

Abstract: Mobile Ad-hoc Network (MANET) routing problems are thoroughly studied several approaches are identified in support of MANET. Improve the Quality of Service (QoS) performance of MANET is achieving higher performance. To reduce this drawback, this paper proposes a new secure routing algorithm based on real-time partial ME (Mobility, energy) approximation. The routing method RRME (Real-time Regional Mobility Energy) divides the whole network into several parts, and each node's various characteristics like mobility and energy are randomly selected neighbors accordingly. It is done in the path discovery phase, estimated to identify and remove malicious nodes. In addition, Trusted Forwarding Factor (TFF) calculates the various nodes based on historical records and other characteristics of multiple nodes. Similarly, the calculated QoS Support Factor (QoSSF) calculating by the Data Forwarding Support (DFS), Throughput Support (TS), and Lifetime Maximization Support (LMS) to any given path. One route was found to implement the path of maximizing MANET QoS based on QoSSF value. Hence the proposed technique produces the QoS based on real-time regional ME feature approximation. The proposed simulation implementation is done by the Network Simulator version 2 (NS2) tool to produce better performance than other methods. It achieved a throughput performance had 98.5% and a routing performance had 98.2%.

Keywords: Mobile ad-hoc network (MANET); routing problem; regional approximation; secure routing; QoS support factor; trusted forwarding factor; data forwarding support (DFS); mobility; energy

1 Introduction

MANET is better for performing data communication with billions of devices among the networks. Various intermediate networks partner keep connecting us. It supports seamless data transmission and includes multiple mobile nodes and fixed base stations. In any group, the presentation depends on how that gives consistent information moved. To provide constant sending, need to identify malignant hubs that interfere with sending and posture different risks. So, must wire it safely. The

presence of malicious nodes involving Threads, including sniffing attacks and modification attacks, affect the overall performance of the MANET, and secure Routing is needed to increase the MANET.

The Routing in MANET is acted in more than one way. In summary, hopping involves a basic approach used in the sense of reducing inertia. At the same time, short-path midpoints are chosen to have maximum flow, and the packet's droplet count increases, ultimately decreasing efficiency. Traffic-based Routing is implemented with a strategy of selecting the path with the minor traffic. Can withstand long jump counts that spread idle and reduce performance.

Additionally, there are a lot of approaches available for Routing. For Secure Mobility, a node's trustworthiness is evaluated locally or globally in various ways. In the primary method, nodes collect information about the rest of the nodes to measure their trust in the media. Additionally, the trust of a node is evaluated by its previous behavior during communication. Anyway, the techniques endure accomplishing better execution in securely routing the information parcels, by taking into account this large number of issues, a productive constant ME estimation based secure directing scheduling.

Consider a network N geographically distributed with X and Y meter intervals. If the source node has to choose a protected path, that path is divided into several districts. Instead of dividing the global space into four parts, each node can form a boundary and divide them into several sections.

Fig. 1 shows an example of source to destination node communication in the MANET network. Here S illustrates source node and D means target node. The proposed technique calculates each node's energy, speed and distance. Suppose deficits have two harmful purposes, including revenge training. For example, consider node N in geographic regions x and y. In this case, we can cover an area of up to 300 m and divide it into four districts. Within this district, nodes can learn and assess behavior according to their diversity and potential.

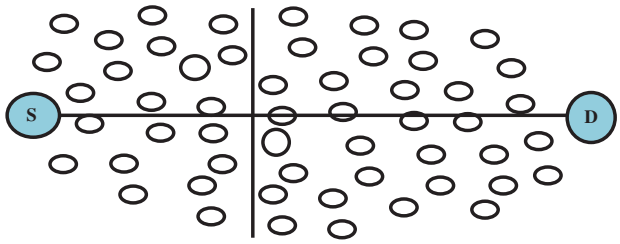

Figure 1: Sample of source to destination communication network

Since the node of interest k is in that space, the transmission in question and the collection of the consumed energy can be approximated without problems. It allows for identifying devastating nodes found within network. By differentiating the presence of malicious nodes within a region, locale nodes avoid communicating through recognized malicious nodes.

Our Contribution

Trusted Forwarding Factor (TFF) calculates the various nodes based on historical records and other characteristics of multiple nodes. Similarly, the calculated QoS Support Factor (QoSSF) calculating by the Data Forwarding Support (DFS), Throughput Support (TS), and Lifetime Maximization Support (LMS) to any given path. One route was found to implement the path of maximizing MANET QoS based on QoSSF value. The proposed RRME technique gives QoS performance during sender and receiver communication on MANET.

2 Literature Survey

The author suggest several directing schedules, and such techniques are portrayed exhaustively in part.

A fuzzy rules-based approach to meet security requirements. It removes the vindictive blade and recognizes those who believe in the way. The proposed calculation improves the performance of MANET [1]. The Mane's handling relies heavily on its steering system. To this end, [2] introduces a standard power-based actuation rule using steering measurements. Consider energy and information transfer methods. Paths are resolved progressively by limits.

Data transmission and execution security in a complex secure estimation to distinguish the dangers impacted an association's presentation [3]. It can see vehicles going the opposite way; in light of that, it would pick a protected course [4]. Explained a safe-coordinated estimation that trades keys. The KEA computation handles various assaults. To build QoS hash based secure directing is created [5]. This technique consolidates security highlights with the current on-demand coordinating calculations. The Dynamic Probabilistic Routing Algorithm was talked about as being energy-proficient. This conventional flooding part produces many duplicate bundles sent around the association, causing an authoritative clash, crash, and retransmission. A probabilistic telecom calculation was utilized to develop the flooding component further and keep storms from communicating across MANETs. The disturbance in the remote channel created an extraordinary probabilistic controlling calculation to adapt to package duplication and mistakes. The number of hubs in the neighborhood MANET climate was considered to work out the retransmission probability [6].

The author expressed AODV protocol based secure communication opposed to block whole attack in MANET [7]. The author implemented an ID-based cryptosystem in [8] to advance security execution. The method uses a hash chain with a meeting key for validation. The learning automata hypothesis has been utilized to resolve a couple of issues. It has been changed for directing in MANET [9], where a mysterious steering strategy with area touchy is introduced, parting the association and assessing the certainty of hubs with adaptability, way disaster, and strength of sign in way assurance. Like [10], a proficient Optimal Decided Trust Inference (ODTI) model is introduced, which picks the communicating hub in view of the neighbors' trust, where that trust has been assessed considering past transmissions.

A tied-down calculation to impede the information [11] and a triple component-based secure guiding estimation [12] measure the trust of hubs given the info got from neighbors to shield against dull opening attacks in MANET. The sending hub was picked utilizing a standing-based guiding estimation where neighborhood eminence is approximated [13]. Secure directing purposes trust measures, and another method called Trust-Based Secure Routing that uses a crossover streamlining calculation has been created. The Dolphin Cat Optimizer is utilized to pick the course, and earlier activities gauge hub trust [14]. Fundamentally, energy-based multicast coordinating with further developed solidness was introduced in [15], distinguishing the dependable way per trust measurements.

The study introduced the Bacteria for Aging Optimization Algorithm (BFOA) and Fuzzy Clustering (FC) methods [16]. The BFOA method analysis the perfect nodes and FC selects CH. Genetic Algorithm (GA) and Fuzzy C-means clustering (FCMC) techniques designed by [17] for secure routing communication. The study aimed to enhance QoS performance in MANET, therefore the study expressed Cat slap single player algorithm and fuzzy logic for secure communication in the network [18]. In reference [19] designed recurrent reward algorithm for secure neighbor node selection based on node behavior in MANET. The novel expressed AAS technique for identify the attacks in MANET [20]. The suggested method produces better PDR performance. Similarly the novel explored

Authenticated Anonymous Secure Routing scheme for opposed to attack in MANET [21]. In [22] introduced secure cross layer routing protocol for MANET analyzing the performance. The creator of [23,24] inspects various guiding shows concerning major security frameworks, adaptability, above, and different elements, including SAR, SEAD, ARAN, and others. In MANET [25], which utilizes both physical and legitimate trust, the trusts of different hubs were used for coordinating. The system uses energy, time, Packets numbers, and signs strength. A superior OLSR calculation with security execution SOLSR was made, which utilizes timestamp values to check the pathways' degree of trust [26]. Presenting a Data Confidential and Reliable Bee Clustering Routing Protocol [27]. The technique utilizes the bundle sending number to distinguish the assault. The author exposes the Blockchain system for Security Data collection (B4SDC) technique for communication sender node to the target node in MANET [28]. In reference [29] study explained Atanassov's Intuitionistic Fuzzy Set (A-IFS) theory to increase the network performance class.

Problem Statement

- Mobile Ad-hoc Network (MANET) is at risk from various attacks, and security depends on several QoS conditions. The alteration and steering assaults are recognized as the most prevailing ones influencing the network's presentation.
- Adversaries can know network traffic and effectively impose scalability on all exchanges by showing that it is the shortest hop to reach the goal and has the most significant potential to contribute to the network's life. The solutions investigated fought against poor results in achieving QoS.

3 Proposed Real Time Regional ME Feature Approximation Based Secure Routing

The proposed secure routing scheme based on real-time partial ME approximation starts from route discovery that collects various information such as location, energy, and related exchanges. Use these to perform ME approximation and choose a way to perform data transfer. Depending on the chosen method, this method will perform the data transfer. Detailed instructions are detailed in this section.

Fig. 2 depicts the functional architecture of the suggested RRME routing system, and this section goes into great depth on each of its available components. The source sent data then the proposed identified route based on Real-time Regional Mobility Energy (RRME). Then evaluate the Trusted Forwarding Factor (TFF) using regional mobility energy. Finally, QoSSF Route Selection is based on the packets received by the destination node.

3.1 RRME Route Discovery

The route finding was carried out by distributing the path solicitation to its neighbors. First, the source node that generated the RRME route requests and broadcasts an RRME-REQ packet to the organization. The nodes that received the RRME-REQ bundle identify the passage in their neighbor and path tables. The RREQ-REP package, which contains the portability speed, area, and several transmissions sent, is produced by any node that recognizes the existence of a route and sends it in the direction of the source node. In any event, the neighbors of the intermediate nodes have received a new broadcast of the RRME-REP package. Finally, accepting the RRME-REP message, the source node focuses on the sequence's list of pathways and the components of the different transitional nodes.

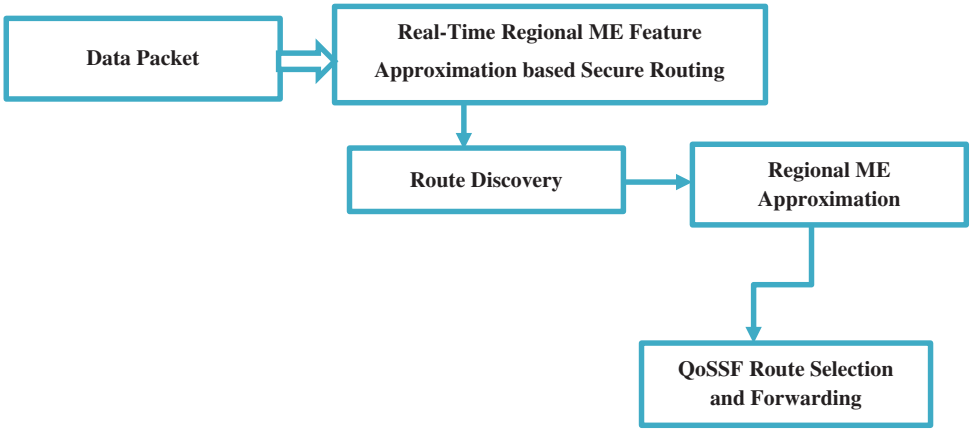

Figure 2: Proposed RRME routing algorithm

Algorithm steps

Input: Route Table RT, Neighbor Table NT
Return: RT, NT
Start
Check Packet P.
Produce RRME-REQ parcel.
Transmission RRME-REQ.
While Transmission Timer Runs
Neighbor gets RRME-REQ parcel.
If chance that $NT\,(Neighbor) \in RRMEREQ\,(Dest.ID)\ ||\ RT\,(Neighbor)\ \in RRME-REQ\,(Dest.ID)$
$Produce\ RRME-REP = \{NodeID,\ Location,\ Speed,\ Energy,\ NOT\}$
Send to source
Else
Broadcast RRME-REQ to neighbors
End
Source gets RRME-REP.
Separate paths and subtleties and add them to the Route table.
$RT = \sum (Routes \in RT) \cup RRMEREP\,(Route,\ Nodeid, speed, location, energy, Not)$
End
Stop

The above computation included the process of path disclosure calculation, which results in an RRME-REQ parcel to determine the path. It isolates various path data, such as nodes' area, energy, flexibility, and speed, by obtaining the solution. The path table, which is used in sequence determination, has distinguished subtleties added to it.

3.2 Regional ME Approximation

In this portion, the approximate locations of the several districts and the routes through the territory are acted. The plan's first step is to divide the entire area into four quarters per the goal. This strategy compiles the list of paths based on where the target is reachable. This method identifies

for each root a list of mobile nodes. Therefore, this method accumulates the strength and speed to evaluate the Trusted Forwarding Factor (TFF). The TFF value identifies a group of sequences; some are eliminated because they are deemed dangerous pathways. Such approximations are used in the subsequent stage's path decision process.

Algorithm steps

Input: Route Table (RT), Network Topology Topo
Output: Route List (RL)
Begin
Step1: Read route table RT.
Read Topo
Step 2: Split the network into four regions.
Region set $Regs$ = split (Topo, 90)
Step 3: Differentiate the district where the objective is established.
Region R = $\int_{p=0}^{size(Regs)} Regs\,(p) \in End$
Gather the paths in the locale R.
Route List $Rls = \sum_{i=1}^{size(RT)} RT(i).Coordinates \in R.coordinates$
For each path, R
Identify list of mobile nodes Men's = $\sum Nodes \in R$
For each node N
Recognize previous logs Nl = $\sum_{i=1}^{size(Traces)} Traces\,(i) \in N$
Compute total transmissions $Tt = size\,(Nl)$.
Compute Mobility Support $Ms = \dfrac{Tt \times speed\,(n)}{size\,(Nl)}$
Compute Energy support $Es = (InitialEnergy - (Tt \times MinEnergy))$
If $Dist((Ms, Location\,(N)\,, Loc\,(N-1))\ \langle Tr \,\&\&\, Es\rangle\ ETh$ *then*
Leave
Else
Break
End if
End if for
TFF = $\sum_{i=1}^{size(R)} R(i).Ms \times R(i).Es$
If TFF> Th, then
Add to route list Rl.
End if
End for
Stop

The above-examined calculation addresses how they believed sending factor has been estimated for various paths distinguished in any district. The technique first determines the rundown of paths in the neighborhood, and for each path, the strategy calculates portability and energy support. In light of these qualities, the technique figures the Trusted Forwarding Factor (TFF), which is utilized to perform path determination.

3.3 QoSSF Route Selection and Data Forwarding

The QoS requirements do the course determination. To complete this activity. The technique initially analyzes the way list recognized in the past stage, liberated from malicious hubs. The methodology does Lifetime Maximization Support (LMS), throughput backing, and information sending support (DFS) for every way LMS. The technique enrolls the QoS Support factor (QoSSF), utilizing these many qualities (QoSSF). Finally, a single method for data transmission is decided upon in light of the value of QoSSF. The chosen path was used to send the information.

Algorithm steps

Start

For any path R, the worth of Data Forwarding support DFS is estimated as follows.

$$\text{DFS} = \frac{\sum_{i=1}^{size(R)} R(i).Mobility < Th}{size\,(R)}$$

Additionally, the throughput support Ts is estimated as follows:

$$\text{Calculate Throughput Support TS} = \frac{\sum_{i=1}^{size(R)} R(i).TotalTransmission}{size\,(R)}$$

The worth of a lifetime boost is estimated as follows:

$$\text{Calculate Lifetime maximization support LMS} = \frac{\sum_{i=1}^{size(R)} R(i).Energy > ETh}{size\,(R)}$$

Utilizing this multitude of values, the QoSSF esteem is estimated as below:

$$\text{Compute QoSSF} = \frac{DFS \times TS}{LMS}$$

Essentially, the worth of QoSSF is estimated for different courses, and on this premise, the system with the biggest QoSSF is chosen for information sending.

End For

Stop

Fig. 3 displays the operation of this system. The map is approximated in terms of mobility and energy to find effective and safe data transport techniques. In this proposed section efficiently communicate sender to receiver node based on Real-time Regional Mobility Energy (RRME).

4 Experimental Results

A network simulator was used to develop and test a hard-coded RRME approximation-based QoS SF routing system, and its performance was assessed. The performance of the suggested technique is evaluated in several simulated settings. This section displays the assessment results.

The information utilized to assess the performance of the suggested RRME algorithm is displayed in Table 1. The following variables evaluate how well these techniques perform:

Under various node settings, the MANET directing performance has been computed and presented in Table 2. The suggested RRMEA computation has produced more incredible directed execution than other methodologies. The assessment is performed using the node counts of 50, 75, and 100. The steering performance in each situation is assessed according to several schedules. According to the results, the suggested RRMEA computation has resulted in more incredible steering execution across all experiments.

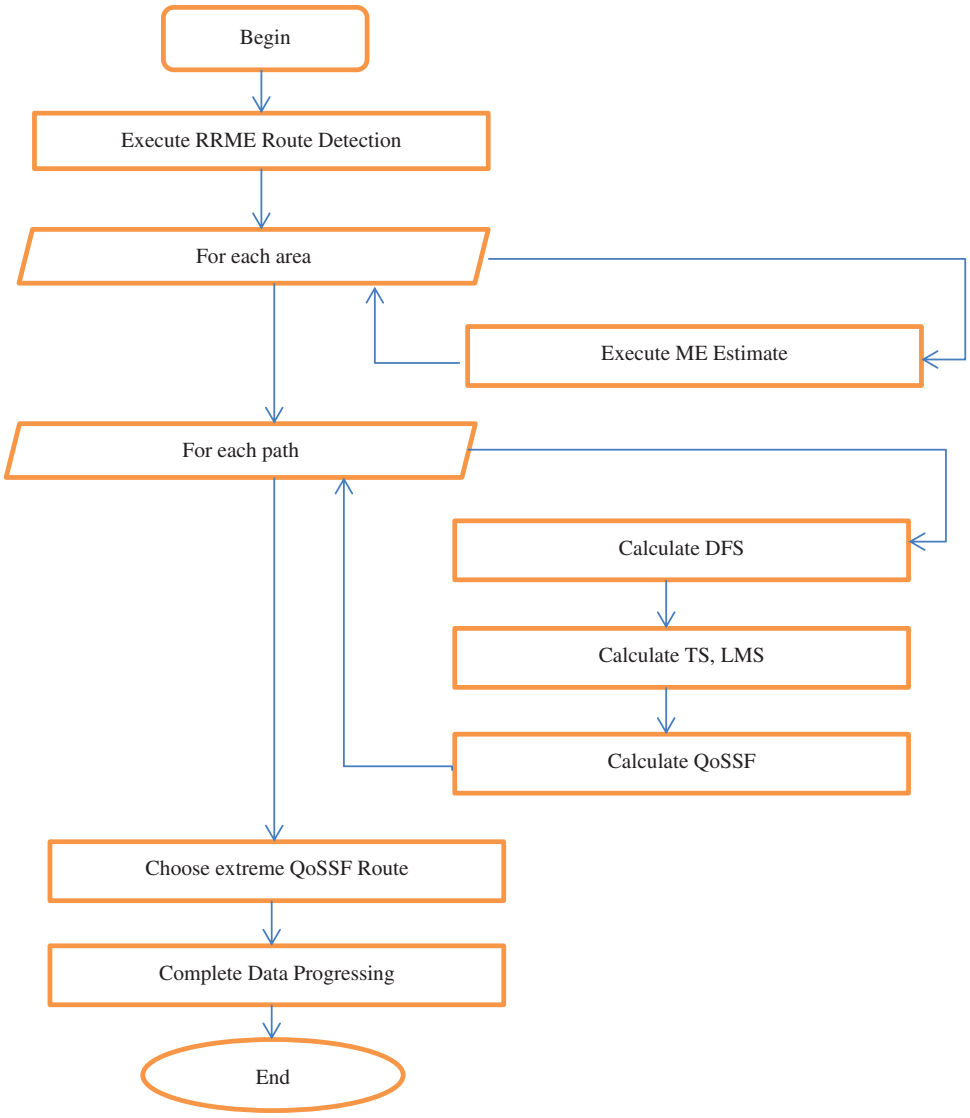

Figure 3: Flow chart of RRME feature calculation based on the routing

Table 1: Simulation parameter settings

Simulation parameters	Simulation value
Simulation tool	Ns2
Number of nodes	100
Communication range	100 m
Power	10 Joules
Time	10 min

Table 2: Performance of routing *vs.* number of nodes

Performance of routing			
Algorithm method	55 Nodes	85 Nodes	100 Nodes
Fuzzy rule in %	66	72	77
Trust based in %	69	76	81
Probabilistic routing in %	73	80	85
MCNFA in %	80	88	97
RRMEA in %	83	92	98.2

The calculated and examined directing performance of various techniques on various nodes is shown in Fig. 4, where the suggested RRMEA strategy results in better guiding execution than other methods. In conditions with 55 nodes, 85 nodes, and 100 nodes, it is clear that the suggested RRMEA technique has achieved greater guiding execution. By altering the node count, the assessment is carried out, and the steering execution is calculated.

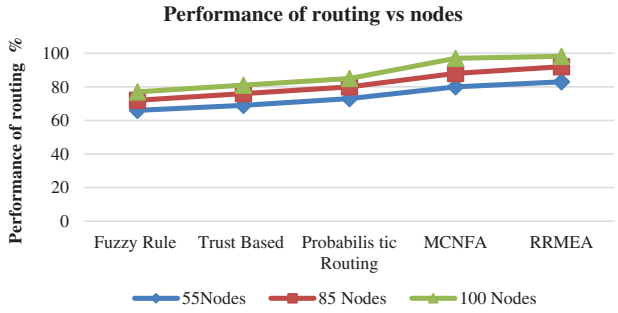

Figure 4: Analysis of routing *vs.* number of nodes

Table 3 estimates and presents the throughput produced by various schedules and shows that the suggested RAMA computation performed better in every situation. A total of 100 nodes, 85 nodes in the geography and 55 in the reproduction, make up the throughput assessment. At each experiment, an estimation and an introduction to the throughput execution of various directing schedules are made. In every trial, the suggested RRMEA computation produced more excellent throughput execution than alternative alternatives.

Fig. 5 estimates and presents the throughput execution produced by various schedules under shifting nodes and shows that the suggested RRMEA calculation has achieved a more excellent throughput execution than multiple techniques. The estimated and shown throughput execution of the approaches at the reenactment of 50, 75, and 100 nodes. The suggested RRMEA computation produced superior throughput execution in each trial compared to other methodologies.

For various methodologies, the number of bundle drops produced by multiple processes has been calculated, and RRMEA computation produces less PDF depending on the situation. The quantity of parcel drops varies depending on how many nodes are present in the reproduction, which would support directing. When more nodes exist, there will be many paths to arrive at any objective that would uphold the steering. The presentation of parcel drop number is approximated and introduced

in Table 4 using the node counts of 55, 85, and 100. The suggested RRMEA plot has produced fewer bundle drop numbers at various reproduction conditions than other schemes.

Table 3: Performance throughput *vs.* number of nodes

Performance of throughput			
Algorithm method	55 Nodes	85 Nodes	100 Nodes
Fuzzy rule in %	63	68	73
Trust based in %	65	72	80
Probabilistic routing in %	72	77	83
MCNFA in %	80	88	97
RRMEA in %	88	94	98.5

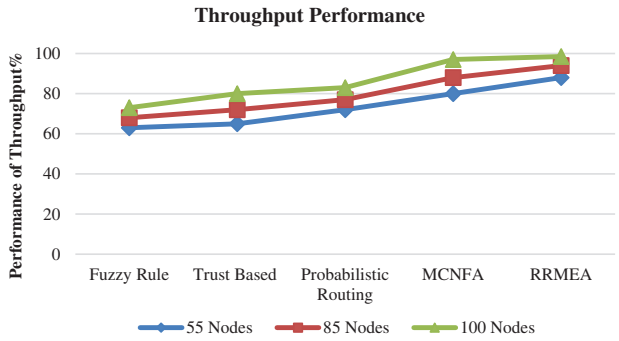

Figure 5: Analysis throughput *vs.* number of nodes

Table 4: Performance packet drop ratio *vs.* number of nodes

PDR in %			
Algorithm method	55 Nodes	85 nodes	100 Nodes
Fuzzy rule in %	36	30	25
Trust based in %	33	26	21
Probabilistic routing in %	29	22	17
MCNFA in %	22	14	5
RRMEA in %	19	12	4

The RRMEA technique provides reduced PDR esteem and estimates the PDR number caused at various node conditions. The quantity of parcel drops varies depending on how many nodes are present in the reproduction, which would support directing. There will be many ways to get to any destination that will help the steering when there are more nodes. The presentation of the drop ratio is approximated and introduced in Fig. 6 using the node counts of 50, 75, and 100. The suggested RRMEA plot has produced fewer bundle drop numbers at various replication conditions than other methods.

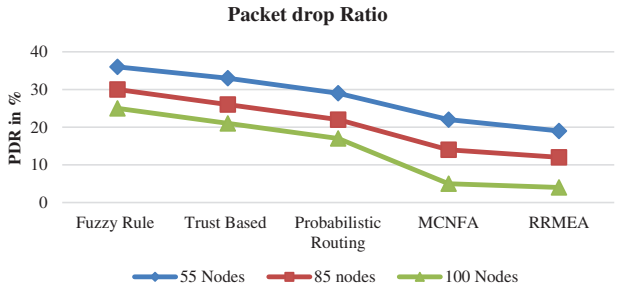

Figure 6: Analysis of packet drop ratio performance

The expected amount of redundancy performance caused by various nodes is listed in Table 5. The suggested RRMEA computation has consistently produced less idleness than alternative solutions in all circumstances. When 55 nodes, 85 nodes, and 100 nodes are engaged in recreation, the idleness assessment is computed at those times. The value of inactivity is assessed for each circumstance and presented in Table 5. In every trial, the suggested RRMEA computation produced less idleness than other methods.

Table 5: Latency *vs.* number of nodes

Latency ratio in milliseconds			
Algorithm method	55 Nodes	85 Nodes	100 Nodes
Fuzzy rule in Ms	96	90	85
Trust based on Ms	83	77	71
Probabilistic routing in Ms	69	62	57
MCNFA in Ms	32	24	15
RRMEA in Ms	23	18	12

Fig. 7 illustrates the lag caused in information transmission at various nodes by various approaches. When there are 50 nodes, 75 nodes, and 100 nodes in the reenactment, the dormancy assessment is estimated. Fig. 7 estimates the value of inactivity in each situation and introduces it. In every trial, the suggested RRMEA computation reduced idleness more than other methods.

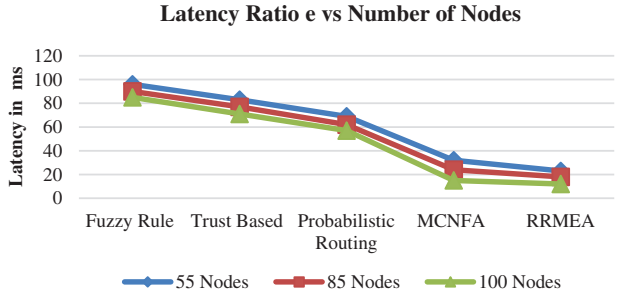

Figure 7: Performance on latency *vs.* number of nodes

The security execution provided by various methodologies has been calculated for various methods, and RRMEA estimates have formed higher security execution in multiple situations. The achievement uses different node layouts such as 50, 75, and 100. Table 6 estimates options in each case. The RRMEA shows high security compared to other methods.

Table 6: Analysis of security *vs.* number of nodes

Security in %			
Algorithm method	55 Nodes	85 Nodes	100 Nodes
Fuzzy rule in %	63	70	75
Trust based in %	67	74	82
Probabilistic routing in %	70	79	85
MCNFA in %	82	86	95
RRMEA in %	88	90	97

Estimates of security performance under various conditions show that RRMEA computation outperforms other methodologies in terms of security. The security execution is evaluated by changing the number of nodes in the reproduction in Fig. 8. At 55 nodes, 85 nodes, and 100 nodes, the construction is done. The suggested RRMEA computation has consistently produced more excellent security execution than alternative methods.

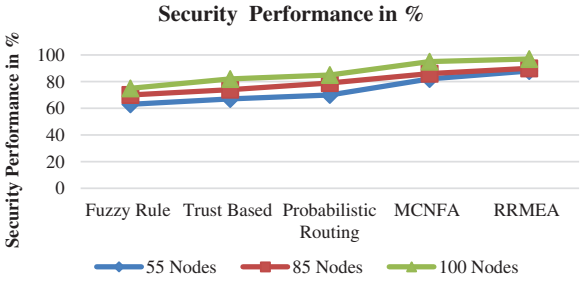

Figure 8: Analysis security *vs.* number of nodes

5 Comparison

This section discusses our proposed RRME algorithm compared with previous Fuzzy Rules, Trust Based, Probabilistic Routing and MCNFA techniques. Our proposed system produces a throughput is 98.5%, a routing performance is 98.2%, a security performance is 97%, a delay performance is 12 ms, and a packet drop ratio is 4% for 100 nodes.

Likewise, the existing Fuzzy Rule achieved 97% of security performance, a throughput performance of 73% and a delay performance is 85 ms. Trust Based method produced 80% throughput performance, 82% security performance and a delay performance is 71 ms. Then Probabilistic Routing achieved 83% of throughput performance, 85 of security performance and delay performance is 5 ms. Also, the MCNFA algorithm attained 97% of throughput performance, 95% of security performance and a delay is 15 ms for 100 nodes.

However, the proposed method provides efficient performance with minimum delay for secure communication in MANET than other methods.

6 Conclusion

This article evaluated a sound continuous provincial versatile energy estimating method to increase QoS in the mobile ad-hoc network. The technique uses path revelation to compile the architecture of routes leading to the target node. The strategy recognizes where the goal is located and divides the organization into several sections. The approach distinguishes how the courses are set up concerning the district. The method calculates the Trusted Forwarding Factor (TFF) for each to identify the presence of a harmful node. A subset of pathways is placed, as shown by the value of TFF. The method records QoSSF esteem for each path identified using information transmission, lifespan amplification, and throughput variables. Finally, a single route successfully transmits information under CSSF standards. The suggested approach reduces the lot drop component more than others and improves the appearance of direction.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] G. Mukesh Kumar, S. Neeta and V. Poonam, "Fuzzy rule-based approach for design and analysis of a trust-based secure routing protocol for MANETs," *Procedia Computer Science*, vol. 132, pp. 653–658, 2018.

[2] S. Sajal and R. Datta, "An adaptive protocol for stable and energy-aware routing in MANETS," *IETE Technical Review*, vol. 34, no. 4, pp. 1–13, 2016.

[3] A. K. Al. Shammari, P. Ehkan and Y. Naimah, "Future barriers challenging security attacks and secure routing issues in MANET," *Australian Journal of Basic and Applied Sciences*, vol. 11, no. 15, pp. 20–25, 2017.

[4] L. Raghavendar Raju and C. R. K. R. Reddy, "A key exchange approach for proficient and secure routing in mobile adhoc networks," *International Journal of Managing Information Technology*, vol. 11, no. 4, pp. 43–54, 2017.

[5] N. Haripriya and N. Rajalakshmi, "An energy efficient dynamic probabilistic routing algorithm for mobile adhoc network," *International Journal of Recent Technology and Engineering*, vol. 7, no. 63, pp. 1699–1707, 2019.

[6] V. Abhishek, "Implementing security features in MANET routing protocols," *International Journal of Computer Science and Network*," vol. 10, no. 8, pp. 51–57, 2018.

[7] A. M. El. Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019.

[8] S. Menaka, "Secured routing deterrent to internal attacks for mobile ad hoc networks," *Journal of Engineering Science and Technology Review,* vol. 11, no. 1, pp. 1–9, 2018.

[9] S. Hao, H. Zhang and M. Song, "A stable and energy-efficient routing algorithm based on learning automata theory for MANET," *Journal of Communications and Information Networks*, vol. 3, no. 2, pp. 43–57, 2018.

[10] M. S. Swetha,"A novel approach to secure mysterious location-based routing for MANET," *International Journal of Innovative Technology and Exploring Engineering*, vol. 7, no. 7, pp. 2587–2591, 2019.

[11] M. Jaganath, "Performance evaluation of MANET routing protocol under black hole attack using opnet simulator," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 398–402, 2019.

[12] R. B. Mohammad, "Secured approach towards reactive routing protocols using triple factor in mobile ad hoc networks," *Annals of Emerging Technologies in Computing*, vol. 3, no. 2, pp. 32–40, 2019.

[13] G. Lenin Delgado, E. Mezher and L. Pallarès-Segarra, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 77, pp. 1–16, 2019.

[14] M. M. Moresh and K. Uttam, "Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm," *The Computer Journal*, vol. 62, no. 10, pp. 1528–1545, 2019.

[15] S. Gopinath, "Energy-based reliable multicast routing protocol for packet forwarding in MANET," *Journal of Applied Research and Technology*, vol. 13, no.3, pp. 374–381, 2015.

[16] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[17] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[18] N. Veeraiah and O. Ibrahim Khalaf, "Trust aware secure energy efficient hybrid protocol for MANET," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.

[19] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou *et al.,* "A recurrent reward based learning technique for secure neighbor selection in mobile ad-hoc networks," *IEEE Access*, vol. 9, pp. 21735–21745, 2021.

[20] J. Tu, D. Tian and Y. Wang, "An active-routing authentication scheme in MANET," *IEEE Access*, vol. 9, pp. 34276–34286, 2021.

[21] W. Liu and M. Yu, "AASR: Authenticated anonymous secure routing for MANETs in adversarial environments," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585–4593, 2014.

[22] A. A. Bhusari, P. M. Jawandhiya and V. M. Thakare, "Analyzing the performance of an optimized secure cross layer routing protocol with secure cross layer routing protocols for mobile adhoc networks," *International Journal of Research in Advent Technology*, vol. 7, no. 2, pp. 605–611, 2019.

[23] A. A. Bhusari, P. M. Jawandhiya and V. M. Thakare, "Optimizing performance of anonymity based secure routing protocol utilizing cross layer design for mobile adhoc networks," in *Fourth Int. Conf. on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, pp. 1–6, 2018.

[24] G. K. Wadhwani, S. K. Khatri and S. K. Muttoo, "Critical evaluation of secure routing protocols for MANET," in *Int. Conf. on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India, pp. 202–206, 2018.

[25] D. Gayathri and S. J. Raman, "Pltrust AODV: Physical logical factor estimated trust embedded AODV for optimized routing in MANETs," in *IEEE, Int. Conf. on Advanced Computing and Communication Systems*, Pune, India, pp. 1–5, 2017.

[26] S. Gadekar and S. Kadam, "Secure optimized link state routing (OLSR) protocol against node isolation attack," in *IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, India, pp. 684–687, 2017.

[27] R. Sajyth and G. Sujatha, "Design of data confidential and reliable bee clustering routing protocol in MANET," *International Journal of Engineering & Technology*, vol. 7, no. 661–666, pp. 1–7, 2018.

[28] G. Liu, H. Dong, Z. Yan, X. Zhou and S. Shimizu, "B4SDC: A blockchain system for security data collection in MANETs," *IEEE Transactions on Big Data*, vol. 8, no. 3, pp. 739–752, 2022.

[29] D. Giveki, H. Rastegar and M. A. Karami, "New neural network classifier based on atanassov's intuitionistic fuzzy Set theory," *Optical Memory and Neural Networks*, vol. 27, pp. 170–182, 2018.