Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.030284
Article

Tech Science Press

An Enhanced Trust-Based Secure Route Protocol for Malicious Node Detection

S. Neelavathy Pari[1,*] and K. Sudharson[2]

[1]Department of Computer Technology, Anna University, Chennai, 600025, India
[2]Department of Information Technology, Velammal Institute of Technology, Chennai, 601204, India
*Corresponding Author: S. Neelavathy Pari. Email: neela@annauniv.edu
Received: 23 March 2022; Accepted: 26 April 2022

Abstract: The protection of ad-hoc networks is becoming a severe concern because of the absence of a central authority. The intensity of the harm largely depends on the attacker's intentions during hostile assaults. As a result, the loss of Information, power, or capacity may occur. The authors propose an Enhanced Trust-Based Secure Route Protocol (ETBSRP) using features extraction. First, the primary and secondary trust characteristics are retrieved and achieved routing using a calculation. The complete trust characteristic obtains by integrating all logical and physical trust from every node. To assure intermediate node trustworthiness, we designed an ETBSRP, and it calculates and certifies each mobile node's reputation and sends packets based on that trust. Connection, honesty, power, and capacity are the four trust characteristics used to calculate node reputation. We categorize Nodes as trustworthy or untrustworthy according to their reputation values. Fool nodes are detached from the routing pathway and cannot communicate. Then, we use the cryptographic functions to ensure more secure data transmission. Finally, we eliminate the untrustworthy nodes from the routing process, and the datagram from the origin are securely sent to the target, increasing throughput by 93.4% and minimizing delay.

Keywords: Ad-hoc network; wireless security; trust management; data Mining; cryptography

1 Introduction

In the current world, wireless transmission technology is critical for transitory communication, and the wireless network connects many ends people via several wireless types of equipment. In addition, wifi gadgets have become much smaller and cheaper in recent decades. A collection of wireless nodes connects to a Mobile Ad hoc Network (MANET), allowing changeable network settings without relying on any underlying architecture [1–4]. Each node in the network has a data transceiver to transmit and receive information. The transceiver's propagation is two-way, allowing users to send and receive via a wireless link. However, the transceiver's capability limits a specific range; it can only interact with nodes within its wireless coverage. The MANET's feature is its ability to maintain communication among multiple parties without infrastructure and enable the users to transfer signals while the nodes are on the movement.

One of the issues with MANET is that the movable node's transmission coverage is constrained. As a result, it can connect with any node well within the transceiver's area. MANET permits two types of connections to fix the issues of transceiver range limitations: single-hop and multi-hop. Direct contact is a hop-by-hop connection in which data is transferred directly among wireless nodes whenever the communicating nodes are inside the transmission range. So when multiple mobile terminals are not under transmission range, indirect contact can be formed [5–7]. In indirect communication, intermediary nodes communicate and exchange messages to interact between pairs of nodes Multi-hop transmission is referred to as indirect communication.

MANET is a wireless connection paradigm that can accommodate the extensive requirements of end-users. Mobile devices in MANET are free to travel in any direction within the designated range or covering the region. The military atmosphere, disaster recovery, and regular road congestion are typical applications of MANET. Fig. 1 depicts the MANET topology, in which a large number of mobile nodes are interconnected remotely to one another. MANETs are extremely sensitive to numerous routing threats by internal nodes due to their open topologies, decentralized nature, and absence of adequate supervision; hence undertook, several studies to increase MANET system security [8–10]. Consequently, connectivity in such dynamic systems has inherent problems compared to standard wireless connections. Conventional routing techniques for ad-hoc systems are ineffective in combating various routing threats.

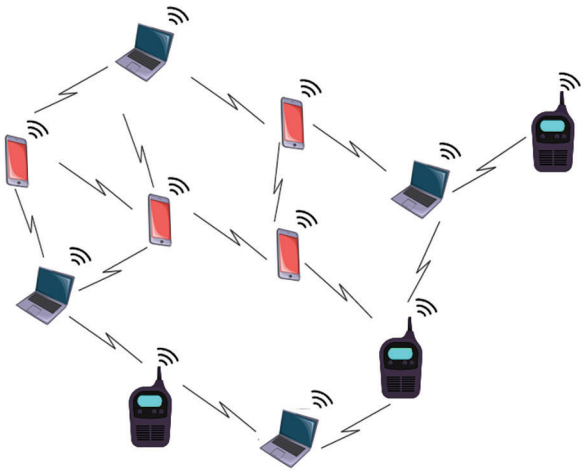

Figure 1: MANET architecture

In MANETs, trust defines a network node's ability to fulfill many other nodes' needs as specified by a core communication system. Each node in a connection controls a separate trust database to calculate and keep the trust level of all other nodes in trust-based security protocols. The estimated reputation scores of the nodes use to make routing information. Even though many studies propose trustworthiness-based solutions in MANETs, practically all suggested solutions struggle with the scaling challenge. A trust-based strategy to establish trust and reputation across network elements takes time. In time-critical situations, such a delay in building trustworthiness is frequently unacceptable. A malfunctioning node will have more opportunities to discard transmissions before being recognized as vicious because of the slowdown in establishing trust [11–13]. Individual node security is crucial in MANET to shield each user's personal information. An attacker may broadcast fraudulent route discovery signals to gain the attention of communicators to attract datagrams, which the attacker then misuses. This research uses features optimization techniques combined with enhanced trust methodologies to allow sensing dangerous nodes in MANET. While all nodes behave selflessly, the connection will perform successfully.

2 Related Works

The research of real-time trustworthy routing protocol for MANETs is ongoing, with efficient trust-based routing being the most critical concern. Routing is selecting routes for datagram transmission in a network. Safety and Quality of Service (QoS) considerations are essential in transmitting packets. This section examines the different routing mechanisms, reputation mechanisms, and data encoding for safe transmissions for MANET.

In a black hole attack, authors [1] developed robust route discovery in AODV. This technique has the benefit of being simple to create and requiring no additional overhead for resource-restricted devices. However, due to these limits, the transmission of data packets is becoming delayed increasingly. In [2], propose an on-demand multicast routing strategy for self-organized networks that is secure and trust-based MANET, highlighting benefits such as these. Improved routing quality and optimized approach to determine the optimum path. However, their study has drawbacks, such as the fact that their suggested protocol can only accept an alternating route with a lower hop count due to the confidentiality requirement. In [3], a secure method of routing protocol for MANET protects the routing system from internal and external assaults. The constraints of their work include the impacts of mobility, which have a significant effect on the performance of MANET. Finally, their paper [4] created a unique successive-hop choice-based secure routing mechanism for wireless ad hoc sensor systems—resilience in the face of several communications from attackers.

The method's limitation is the increased route length. For Mobile Ad-hoc Networks, the researchers designed combined key management and secured routing system [5]. The system is more secure because node-specific broadcast keys are used instead of a single group broadcast key. However, node monitoring is not in the suggested framework. In paper [6], designed and published a topology-based routing system for ad-hoc networks with unpredictable topologies, and their work can provide more excellent performance in terms of node use frequency. However, their technique also has the drawback of not being suitable for more extensive networks. In their study, A Reputation Management Platform for Ad-Hoc Network Data Plane Security, its trust evaluation technology protects the data plane of ad-hoc systems effectively and efficiently. However, this technique has a drawback: the number of attack and vulnerable nodes should be below the number of legitimate nodes [7].

The author uses the proposed power and trust-aware routing procedure to offer a Trust-based secure routing system built upon the suggested Dolphin Cat Optimizer uses the Advanced Encryption Standard (AES-TDCO) [8]. The best path is determined using a projected objective model that focuses on trust factors, current and recorded trust, primary and secondary trust, latency, length, connection lifetime, and connection life span. In addition, the suggested framework combines Dolphin Echolocation with the Cat Swarm Optimization technique to achieve faster global convergence. As a result, the recommended routing protocol achieved the highest throughput, shortest delay, and lowest packet drop and detection rate in a simulation with 75 nodes.

In [9], the author provides a complete security study of MANET routing and proposes effective security architecture for detecting and isolating black holes, wormholes, and attacks from the network's gray hole. These assaults cause more damage to the ad-hoc network during the routing process than any other attacks in the environment. In addition, the study provides an effective detection technique based on three QoS parameters: shortest path, trustworthiness rate, and a capability-based procedure. Furthermore, the suggested approach employs a countermeasure in each node based on the threshold limit to ensure the network's communication among nodes is protected. Moreover, the thresholding contributes to establishing trustworthiness among all connected nodes. As a result, the transmission medium can maintain a secure connection with either the transmitter or the receiver node; this technique provides a high-security environment. Furthermore, safe routing strategies such as trust-based secure routing

protocol (TSRM), cognitive energy-efficient trusted routing methodology (CEMT), and trust-aware routing framework verifies performance, delivery ratio rate, and latency. Finally, relying on the result of this research, they implemented a trusted-based routing system capable of successfully separating network threats such as black holes, wormholes, and other attacks like gray-hole in the system.

In paper [10] describes an intelligent energy-aware strategy for wireless sensor networks that employ smart rules and standard classification to make routing decisions effectively. The fuzzy clustering method utilizes energy-efficient routing with intelligent rules [11]. This method allows for secure communication while also being energy efficient. The authors of [12] address the security difficulties by presenting the Jaya Cuckoo Search (JCS) method, a mixture of the Jaya and Cuckoo Search algorithms for beginning safe routes with MANET nodes, ensuring that the pathway reached is viable and secure. The JCS method employs a multi-objective fitness function that evaluates distance, link life span, latency, power, trust, and reputation to pick a secure pathway. TBSMR, a trust-based multi-path routing system, was proposed in [13] to increase the MANET's overall effectiveness. The recommended protocol discusses congestion management, packet drop minimization, attacker node discovery, and safe data transfer features that the suggested protocol examines to enhance the MANET's QoS. The Bacteria for Aging Optimization Algorithm (BFOA) is used in [14] to provide trust-based secure, and power-aware navigation in MANETs. This algorithm selects the best hops in advancing the routing. Finally, they start the clustering-based process, and Cluster Heads (CH) are picked based on how much implicit, primary, and current trustworthiness each CH has. Furthermore, value nodes were investigated based on trust levels. The CH is also engaged in multi-hop forwarding. The estimated method determines the optimum route, which considers delay, performance, and connectivity only within the circuit's boundaries when selecting the best path.

3 Proposed Work

We have improved the node extraction phase in our suggested work by applying Node-feature Mining and increased trust-based computation to determine the reputation of its neighboring nodes rather than relying just on data transmission (send and receive). However, all node conditions, such as queuing congestion, broken links, and power loss, will be factored in. Our proposal aims to find and isolate the harmful node; hence our process is divided into three stages: (Node-feature Mining, Fine-Tuning, and Trust-based route discovery).

3.1 System Model

The ETBSRP mechanism's operating flow depicts in Figs. 2 and 3. Fig. 2 illustrates The ETBSRP mechanism's training module, and It retrieves the properties of a well-known MANET's trusted and harmful nodes in the system's training phase. These characteristics are enhanced for intrusion detection and safe routing in MANETs accuracy to the utmost level for the attacker node detection procedure utilizing a reputation computation. Fig. 3 shows the recommended system's testing model. The obtained features from each node inside the system's testing phase and all these characteristics are categorized using the trained patterns [15–17]. Trust-based intrusion detection using a Node-feature Mining strategy is provided in this paper to successfully detect selfishness or harmful nodes in the network immediately on. Moreover, the logical and physical measurements are taken into account when assessing the total truthfulness of any mobile node.

3.2 Node-Feature Mining

Fig. 4 depicts the assessment of the trust model on x by z or via node y. First, the primary and secondary features are retrieved, and we calculate the trustworthiness of node values individually. The adjacent nodes over node 'y' are y1, y2, y3, y4, y, and z if the features retrieve from node 'x.'

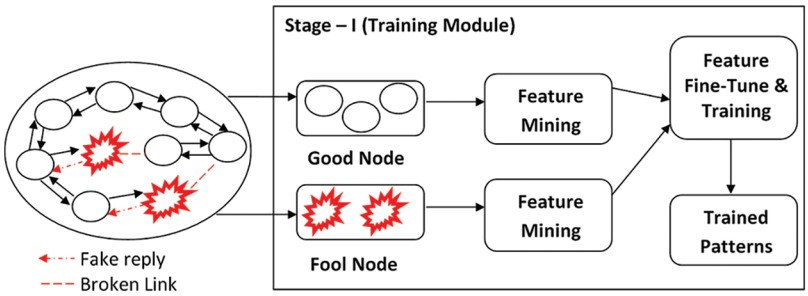

Figure 2: Training module

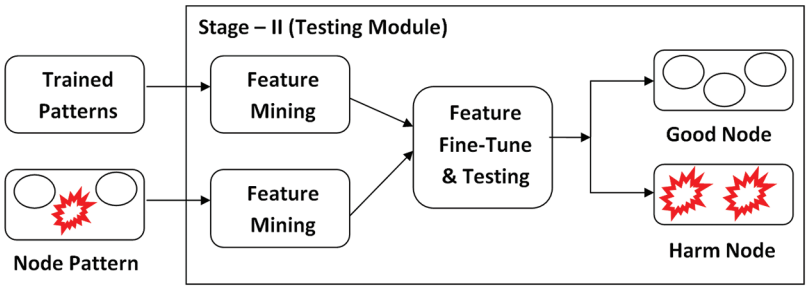

Figure 3: Testing module

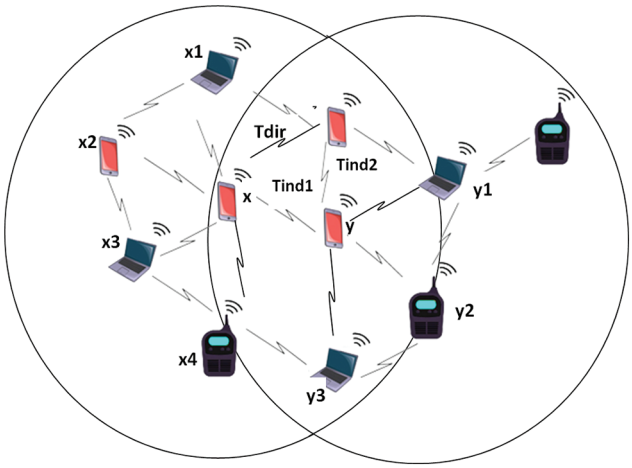

Figure 4: Trust assessment model

In Eq. (1), we estimate the direct trust (Tdir) value as follows:

$$\boldsymbol{T_{dir}} = Pi.\sum_{i=1}^{n1}(Tc_i - \mu)^2.\varphi(t_i) \tag{1}$$

where Pi represents the probability metric as in Eq. (2), Tci represents a number of transactions completed by node 'x' (or) number of positive transactions by 'x' to 'z,' μ is the mean of all ratings of x by z, and φ(ti) = exp ([tn-ti/T]) is the time delay coefficient, where ti denotes the time of i-th interaction (i.e., current transaction), tn indicates the time of n-th interaction, and T is the time.

$$\mathrm{Pi} = \frac{\omega \mathrm{i} - \rho \mathrm{i}}{\omega \mathrm{i}} * \mathrm{T} \tag{2}$$

where ωi is the number of datagram packets recovered over time, 'T' and ρi is the number of datagram packets communicated over the time 'T.'

We calculate the indirect trust estimation by using Eqs. (3), (4), (5), and (6) as follows:

So, the indirect trust estimation between nodes 'x' and 'y' is,

$$\mathrm{T_{ind1}} = \mathrm{Pi} \cdot \sum_{\mathrm{i}=1}^{\mathrm{n1}} (\mathrm{Tc_i} - \mu)^2 . \varphi(\mathrm{t_i}) . \mathrm{wi} \tag{3}$$

where n1 is the number of adjacent nodes over the node 'y.' wi is the weight of an individual node concerning node 'y' as in Eq. (4) as follows,

$$\mathrm{wi} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} Pi \, . \mathrm{Cx} \, . \mathrm{Cy}}{\Sigma Pi} \tag{4}$$

Cx and Cy's creditability represent the interaction event's weight between node 'x' and 'y'.

The trust estimation between nodes 'y' and 'z' is,

$$\mathrm{T_{ind2}} = \mathrm{Pi} \cdot \sum_{\mathrm{i}=1}^{\mathrm{n2}} (\mathrm{Tc_i} - \mu)^2 . \varphi(\mathrm{t_i}) . \mathrm{wi} \tag{5}$$

where n2 is the number of adjacent nodes over the node 'z.'

Now, we calculate the overall neighboring trust as follows,

$$\mathrm{T_{ind}} = \mathrm{T_{ind1}} + \mathrm{T_{ind2}} \tag{6}$$

Hence, the estimation of the reputation of the individual node 'x' is as follows in Eq. (7),

$$\mathrm{R_x} = \mathrm{T_{dir}} + \mathrm{T_{ind}} \tag{7}$$

3.3 Feature Fine-Tuning

The derived features are fine-tune using the techniques below to increase the attacker node detection accuracy.

The following is how our feature fine-tuning methodology performs:

Step 1: Establish the network capacity, connectivity, credibility, and power of each node; then, for fine-tuning, set all of these characteristics.

Step 2: The node community can be formed by,

Xi = {x1; x2; x3…xn}T

Where n represents the number of nodes within the network or node-list, and x is the set of nodes.

Step 3: Using the calculations below shown in Eq. (8), estimate the capacity of each node in a network.

$$\mathrm{Cx} = \sum_{\mathrm{m}=1}^{\mathrm{n}-1} (\mathrm{x_m} - \overline{\mathrm{x_m}})^2 \tag{8}$$

where Cx denotes the capacity of node x, n represents the number of nodes in a network or node-list, and xm denotes the node-mean.

Step 4: Keep updating each node's capacity as 'Cmax' to all other nodes within the network.

Step 5: Keep updating each node's connection reputation value as 'Rmax' additional nodes in the network.

Step 6: To calculate the fine-tune measure; use the following expression as in Eq. (9):

$$Fx = \sum_{m=1}^{n} \left(\frac{C_x - C_m}{C_x} \right)^2 \tag{9}$$

Ca is the mean Capacity of node x, while Fx is the Fine-Tune metric.

Step 7: Keep track of each node's current reputation and capacities in the network node-list and repeat steps 1 through 5.

3.4 Enhancing Trust

ETBSRP is used to expand any reactive routing system, but we choose the ad-hoc on-demand distance vector (AODV) protocol. We enhance the capabilities of AODV following changes outlined in [13] to achieve better routing named Enhanced AODV (EAODV). In addition, we consider adding the components to the neighbor table: (i) power consumption, (ii) affinities, (iii) node bandwidth, and (iv) trustworthiness.

3.4.1 Physical Trust (Power Calculation)

We consider power and bandwidth numbers to forecast physical trust ratings. A node's present power consumption should be adequate to endure full-duplex communication for an extended period. A node's power level is initially high. The power level reduces after the node executes its intended task. Before commencing the information transfer, the transmission power of the nodes captures to determine its dependability. The trusted node 'x' (which evaluates the trustworthiness) obtains the transmission power of the trustee node 'y' (whose trust is to be rated) at the time 'T' as $Pr_{x,y}(T)$. The total data packets multiplied by the ideal power consumption and the node's receive, processing, and sending power consumption for each message yields the power needed for efficient transmission, as shown in Eq. (10).

$$Pr(t) = IP + (RPr, TPr, PPr) * N \tag{10}$$

where N, RPr, SPr, PPr are the number of packets in an interaction, receiving, sending, and processing power requirements by a node for every packet, respectively.

$Pr_{x,y}(T)$ must be bigger than Pr(T) for interaction to be successful. We measure bandwidth using The number of messages delivered at a particular time. The larger the bandwidth, the more packets are routed. As a result, bandwidth is a critical factor in determining the QoS of every network path. Before measuring, the topology refers to the physical trust, which should ensure the data transfer rate between any pair of nodes. At the time 'T,' the attainable bandwidth on the connection (x, y) is approximated as $B_{x,y}(T)$.

3.4.2 Logical Trust

In the logical trust value forecast, we examine closeness and trustworthiness values. The number of prior transactions between a trusted node 'x' and the trustee node 'y' determines the closeness value. The closeness value is initially zero. Suppose a node 'x' in the network sends the packet to a neighboring node 'y'. If the packet passes by node 'x' and node 'y' satisfactorily reaches the endpoint, node 'x' raises node 'y' closeness by one. The acknowledgment sent by the endpoint confirms effective interaction. Alternatively, the score is

lowered by −1 if it does not confirm the interaction. After a specific transaction amount, we estimate closeness as $Cl_{x,y}(T)$ at the time 'T.' When a node enters and exits the network in response to a valid request, the trustworthiness value is increased by +1. However, if a node abruptly departs the network without notice, the node's trustworthiness rating is reduced by −1. Therefore, we estimate trustworthiness as $Ts_{x,y}(T)$ at a given time T, the node 'x' evaluates the trustworthiness of a node 'y'. For example, Eq. (11) defines Reputation(R) at the time 'T' based on the power, bandwidth, closeness, and trustworthiness of the node 'y'.

$$R_{x,y}(T) = \sum_{i=1}^{N} Pr_{x,y}(T) + B_{x,y}(T) + Cl_{x,y}(T) + Ts_{x,y}(T) \tag{11}$$

It is identified as an untrusted node if the overall Reputation value $R_{x,y}(T)$ is less than the predetermined threshold. However, it designates as the communication's trustworthy node.

3.4.3 Enhance Trust Based Routing

The trust value for every node's 1-Hop neighbor is estimated, categorizing nodes as reputable or dishonest after determining trust. Only certified nodes build a path to a destination to establish secure data transmission and exclude the untrustworthy nodes from the transmission channel. Using EAODV routing, the originating node starts the route discovery process. The EAODV routing algorithm may discover several paths to the endpoint, and the sender chooses the path with the highest trustworthiness rating from the various routes supplied to the endpoint. Intermediate nodes, meanwhile, select a new hop with the highest total reputation score and send data along the path. The node's trust value is refreshed on demand when required for data transmission.

3.4.4 Key Generation

The secret key is disseminated between the transmitter and receiver, increasing the security of data transmission. For key exchange, it employs the Elliptic Curve Algorithm. It is a way of transferring cryptographic keys that is unique. It allows a node on the network to communicate securely by sharing cryptographic keys. The shared key is calculated at the two endpoints using elliptic curve cryptography (ECC), and the ciphertext transfers using the key exchange for communicating data [18–22]. The sender encrypts the data and sends this to the next hop using a secret key. This data transmission procedure repeats until the data arrives at its destination. Then, it shares a shared secret key to encrypt and decrypt the data.

4 Performance Analysis

Tab. 1 shows the simulation setup for performance evaluation. We compare the effectiveness of our ETBSRP protocols to that of existing techniques such as TBSMR and BFOA. Our proposed technique study demonstrates how useful it is to employ the following significant QoS criteria based on performance parameters [23–26]. With or without fool node, all current approaches to inquiries compare to the suggested technique based on different standards: latency, energy, throughput, and overhead.

In Tab. 2, the packet delivery ratio (PDR) is the proportion of datagrams delivered by a source node to packets received at the endpoint. The data plane and control packet discarding and attacks employed with the enemy node count set to 20% of the overall number of deployed nodes. The influence of node mobility velocity on the PDR is shown in Fig. 5, while an average throughput is maintained fixed at 4 kbps.

Table 1: Simulation setup

Parameter	Value
Coverage area	1200 * 1200 m
Communication range of each node	250 m
MAC layer protocol	IEEE 802.11
Packet size	512 bytes
Traffic type	CBR-UDP
Channel bandwidth	2 Mbps
Simulation duration	240 s
Mobility model	Random way point
Maximum mobility (varying)	5–25 m/s
Number of nodes	200
Initial energy	750 J
Pause time	4 s
Routing protocols	EAODV, TBSMR, BOFA
Percentage of malicious nodes (varying)	0–40%
Transmit power	1.7 W
Receive power	1.5 W

Table 2: PDR of existing *vs.* proposed ETBSRP approach

PDR (%)			
Number of Nodes	TBSMR	BFOA	Proposed ETBSRP
10	92	90	94
50	90	91	92.5
100	89.5	88	91
150	87	85	90.5
200	86.4	82.5	90.7

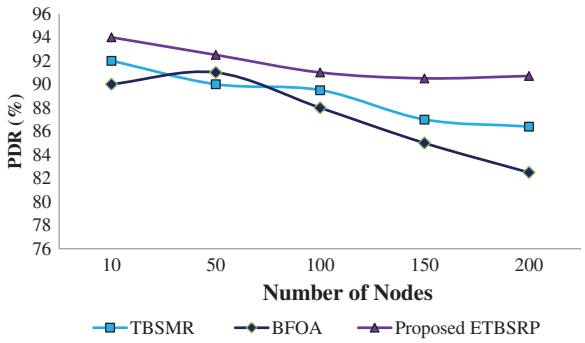

Figure 5: Comparison of PDR

It can show that the ETBSRP has a higher PDR than the TBSMR and BFOA because it separates faulty nodes from directing routes much sooner. Furthermore, the PDR drops significantly as the increase in the number of nodes [27,28]. The explanation for this tendency is that when the node velocity and the number of nodes increase, the node discards packets owing to frequent link disruptions. These findings show that the ETBSRP removes faulty nodes from the network on time and increases the PDR by 2–4% for varied mobility rates and node counts.

Fig. 6 and Tab. 3 show the performance outcome of the TBSMR, BFOA, and ETBSRP procedures. ETBSRP has a more excellent throughput value than TBSMR and BFOA. The ETBSRP technique has a throughput of 518 kbps on average, while the TBSMR and BFOA protocols have 484 kbps.

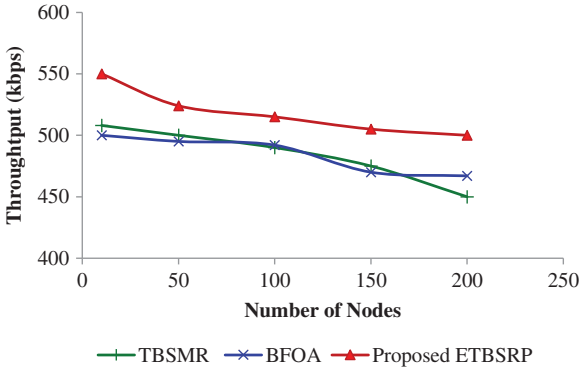

Figure 6: Comparison of performance

Table 3: Performance/throughput

Throughput (kbps)			
Number of Nodes	TBSMR	BFOA	Proposed ETBSRP
10	508	500	550
50	500	495	524
100	490	492	515
150	475	470	505
200	450	467	500

When there is an attack, the performance in ETBSRP decreases while the network size increases due to the rebroadcasting of fraudulent requests. The attacking node will cause a traffic load, which will result in periodic messages being dropped or delayed, affecting throughput and PDR. Under node threat, ETBSRP has slightly more outstanding performance than TBSMR and BFOA but a reduced performance than ETBSRP without node assault.

TBSMR and BFOA have a much more significant average end-to-end (E2E) latency than ETBSRP, as indicated in Tab. 4, the link between E2E delay and the network size displayed in Fig. 7. Because each node sends datagrams directly to the trust-able node, it significantly reduces the average E2E delay of each node in ETBSRP.

Table 4: Average E2E delay

Avg. E2E Delay (ms)			
Number of Nodes	TBSMR	BFOA	Proposed ETBSRP
10	10	11	8
50	15	17	12
100	18	20	14.5
150	20	26	16.2
200	25	35	17.75

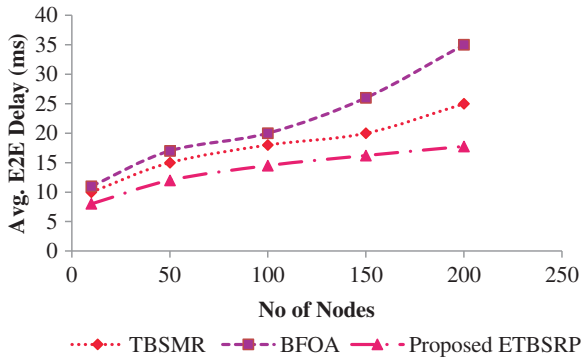

Figure 7: Comparison of E2E delay

ETBSRP also avoids cyclical transfer to reduce average E2E latency. When TBSMR or BFOA cannot locate a suitable friendly node before delivering the datagram, it will disseminate the request packet continuously until it encounters an applicable trust node, improving the average end-to-end latency of network nodes. On the other hand, BFOA has a longer average E2E latency than TBSMR. This justification is that BFOA broadcasts probing packets continuously until it finds a suitable friendly node. Still, TBSMR picks trust nodes by changing each node at an increased power level to reduce the average end-to-end latency of trust-able nodes.

As demonstrated in Fig. 8 and Tab. 5, the Route Overhead (RO) of BFOA grows from about 4.82 to 9.87 as the node velocity increases. However, the TBSMR outperforms the BFOA by decreasing the RO from roughly 3.53 to 7.54; consequently, the resulting RO is larger than ETBSRP, ranging from 2.92 to 4.75.

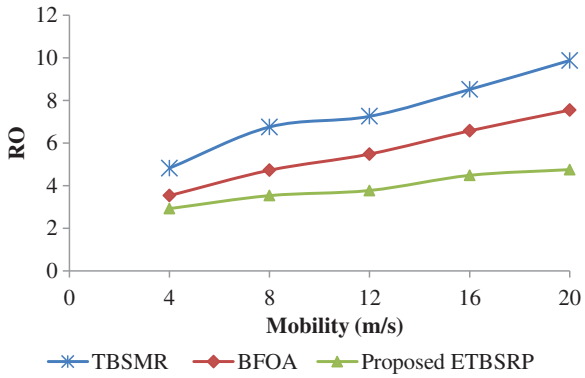

Figure 8: Comparison of RO

Table 5: Routing overhead (RO)

RO			
Number of Nodes	TBSMR	BFOA	Proposed ETBSRP
4	4.82	3.53	2.92
8	6.75	4.72	3.53
12	7.25	5.48	3.77
16	8.51	6.57	4.48
20	9.87	7.54	4.75

Conversely, ETBSRP improves RO by an aggregate of 2.13 compared to TBSMR and BFOA. Furthermore, ETBSRP includes two additional elements in the overall trust and an improved routing method, and it results in fewer routes hand-off procedures than TBSMR and BFOA.

In Tab. 6, the average energy consumption for the MANET adopting TBSMR under Intrusion fluctuates between 303.82 and 320.32 J, as illustrated in Fig. 9. However, in the existence of enemies, ETBSRP boosts TBSMR's energy consumption by an average of 2.73 J.

Table 6: Average energy consumption (J)

Energy Consumption			
Number of Nodes	TBSMR	BFOA	Proposed ETBSRP
0	303.8	302.9	301.1
10	311.2	309.5	306.6
20	314.5	314.15	312.8
30	318.7	316.7	314.93
40	320.32	321.5	319.4

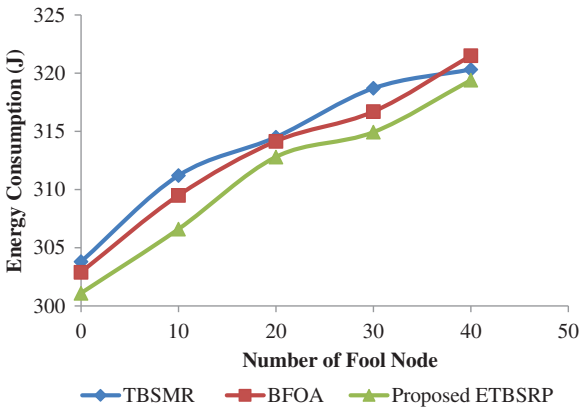

Figure 9: Comparison of average energy consumption

On the other hand, the MANET utilizing BFOA under Attack has an average energy consumption ranging from 302.9 to 321.5 J. Conversely, in the presence of enemies, ETBSRP increases the energy consumption of BFOA by an average of 1.9 J. It powerfully shows that our proposed system outperforms the other procedures.

5 Conclusions and Future Scope

ETBSRP was developed as a routing algorithm to enhance MANET QoS in this work. It is suitable for other wide-ranging networks and considers multiple parameters like traffic, node trust levels, and node battery capacity throughout the routing process, resulting in improved performance and lower overhead. Furthermore, this suggested protocol allows multi-hop routing, which reduces the number of unwanted control packets floating around during route formation in the event of traffic or node malfunction. By detecting malicious nodes, the protocol also assures a secure connection. Our approach finding shows that the proposed ETBSRP protocol beats existing routing strategies in PLR, PDR, average E2E delay, and throughput. Overall, the suggested ETBSRP routing method improves the MANET's QoS and provides cryptographically safe communication. In the fortune, we will focus on implementing security algorithms that incorporate enhanced encryption, decryption, and blockchain technologies to ensure MANET's strong security.

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

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

References

[1] H. Alrahhal, R. Jamous, R. Ramadan, A. M. Alayba and K. Yadav, "Utilising acknowledge for the trust in wireless sensor networks," *Applied Sciences*, vol. 12, no. 4, p. 2045, 2022.

[2] L. E. Jim, N. Islam and M. A. Gregory, "Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes," *Computers and Security*, vol. 113, no. 5, p. 102538, 2022.

[3] J. Rajeshwar and G. Narsimha, "Secure way routing protocol for mobile ad hoc network," *Wireless Networks*, vol. 23, no. 2, pp. 345–354, 2017.

[4] A. Kumar, V. Kumar and K. Kumar, "A novel next hop selection based secure routing for wireless ad hoc sensor networks," *CSI Transactions on ICT*, vol. 4, no. 2–4, pp. 47–53, 2016.

[5] S. Zhao, R. Kent and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1046–1061, 2013.

[6] J. Shen, C. Wang, A. Wang, X. Sun, S. Moh *et al.,* "Organized topology based routing protocol in incompletely predictable ad-hoc networks," *Computer Communications*, vol. 99, no. 2, pp. 107–118, 2017.

[7] S. Tan, X. Li and Q. Dong, "A trust management system for securing data plane of ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7579–7592, 2016.

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

[9] S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: mitigation methods and trust-based approaches," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186–4210, 2021.

[10] K. Selvakumar, L. Sairamesh and A. Kannan, "An intelligent energy aware secured algorithm for routing in wireless sensor networks," *Wireless Personal Communications*, vol. 96, no. 3, pp. 4781–4798, 2017.

[11] P. Kosmides, L. Lambrinos, V. Asthenopoulos, K. Demestichas and E. Adamopoulou, "A clustering based approach for energy efficient routing," in *2016 IEEE Symp. on Computers and Communication (ISCC)*, Messina, Italy, pp. 232–237, 2016.

[12] Ch. Ram Mohan and V. Reddy Ananthula, "Reputation-based secure routing protocol in mobile ad-hoc network using jaya cuckoo optimization," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 10, no. 3, pp. 1–24, 2019.

[13] M. Sirajuddin, Ch. Rupa, C. Iwendi and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QOS of the mobile ad hoc network," *Security and Communication Networks*, vol. 2021, pp. 1–9, 2021.

[14] 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.

[15] N. Partheeban, K. Sudharson and P. J. Sathish Kumar, "SPEC-serial property based encryption for cloud," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23702–23710, 2016.

[16] K. Sudharson, A. M. Ali and N. Partheeban, "NUITECH – Natural user interface technique foremulating computer hardware," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23598–23606, 2016.

[17] J. Aruna Jasmine, V. Nisha Jenipher, J. S. Richard Jimreeves, K. Ravindran and D. Dhinakaran, "A traceability set up using digitalization of data and accessibility," in *3rd Int. Conf. on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, pp. 907–910, 2020.

[18] D. Dhinakaran and P. M. Joe Prathap, "Ensuring privacy of data and mined results of data possessor in collaborative ARM," in *Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems*. Vol. 317. Singapore: Springer, 2022.

[19] S. Arun and K. Sudharson, "DEFECT: discover and eradicate fool around node in emergency network using combinatorial techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 1–12, 2020.

[20] K. Sudharson and V. Parthipan, "A Survey on ATTACK – Anti terrorism technique for adhoc using clustering and knowledge extraction," in *Advances in Computer Science and Information Technology. Computer Science and Engineering. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Berlin, Heidelberg, Springer, vol. 85, pp. 508–514, 2012.

[21] K. Sudharson and V. Parthipan, "SOPE: Self-organized protocol for evaluating trust in MANET using eigen trust algorithm," in *3rd Int. Conf. on Electronics Computer Technology*, Kanyakumari, India, pp. 155–159, 2011.

[22] N. Suganthi and S. Neelavathy Pari, "Detecting malicious nodes in MANET using rateless codes for maximum content distribution," in *Sixth Int. Conf. on Advanced Computing (ICoAC)*, Chennai, India, pp. 308–311, 2014.

[23] M. Sathish, K. Arumugam, S. Neelavathy Pari and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 2040–2044, 2016.

[24] S. Neelavathy Pari, S. Jayapal and S. Duraisamy, "A trust system in manet with secure key authentication mechanism," in *2012 Int. Conf. on Recent Trends in Information Technology*, Chennai, India, pp. 261–265, 2012.

[25] S. Neelavathy Pari, M. Sathish and K. Arumugam, "An energy-efficient and reliable depth-based routing protocol for underwater wireless sensor network (ER-DBR)," in *Advances in Power Systems and Energy Management. Lecture Notes in Electrical Engineering*, A. Garg, A. Bhoi, P. Sanjeevikumar, K. Kamani (eds.), Vol. 436. Singapore: Springer, 2018.

[26] S. Neelavathy Pari and D. Sridharan, "Design of cross layered security architecture to mitigate misbehaving nodes in self-defending network," *European Journal of Scientific Research*, vol. 77, no. 1, pp. 37–45, 2012.

[27] J. Kumar, M. Kulkarni, D. Gupta and S. Indu, "Secure route discovery in AODV in presence of blackhole attack," *CSI Transactions on ICT*, vol. 3, no. 2, pp. 91–98, 2015.

[28] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," *Wireless Networks*, vol. 23, no. 8, pp. 2455–2472, 2017.