

Research Article

TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network

Mohammad Sirajuddin,¹ Ch. Rupa ,² Celestine Iwendi ,³ and Cresantus Biamba ⁴

¹Department of C. S. E., KHIT, JNTUK, Kakinada 522019, India

²Department of C. S. E., V. R. Siddhartha Engineering College, Vijayawada 520007, India

³Department of Computer Science, Coal City University, Enugu 400231, Nigeria

⁴Department of Educational Sciences, Faculty of Education and Business Studies, University of Gavle, 80176 Gavle, Sweden

Correspondence should be addressed to Cresantus Biamba; cresantus.biamba@hig.se

Received 27 February 2021; Revised 28 March 2021; Accepted 8 April 2021; Published 21 April 2021

Academic Editor: Muhammad Shafiq

Copyright © 2021 Mohammad Sirajuddin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobile ad hoc network (MANET) is a miscellany of versatile nodes that communicate without any fixed physical framework. MANETs gained popularity due to various notable features like dynamic topology, rapid setup, multihop data transmission, and so on. These prominent features make MANETs suitable for many real-time applications like environmental monitoring, disaster management, and covert and combat operations. Moreover, MANETs can also be integrated with emerging technologies like cloud computing, IoT, and machine learning algorithms to achieve the vision of Industry 4.0. All MANET-based sensitive real-time applications require secure and reliable data transmission that must meet the required QoS. In MANET, achieving secure and energy-efficient data transmission is a challenging task. To accomplish such challenging objectives, it is necessary to design a secure routing protocol that enhances the MANET's QoS. In this paper, we proposed a trust-based multipath routing protocol called TBSMR to enhance the MANET's overall performance. The main strength of the proposed protocol is that it considers multiple factors like congestion control, packet loss reduction, malicious node detection, and secure data transmission to intensify the MANET's QoS. The performance of the proposed protocol is analyzed through the simulation in NS2. Our simulation results justify that the proposed routing protocol exhibits superior performance than the existing approaches.

1. Introduction

Mobile ad hoc network (MANET) is an assortment of mobile nodes that communicate without any fixed physical framework. MANETs have many striking features like varying topology, rapid setup, and multihop wireless communication. All these features make MANET suitable for various time-sensitive applications [1, 2]. Ad hoc network renders a promising communication facility where physical infrastructure is difficult to establish. Furthermore, MANETs allow mobile nodes to exchange information without any physical framework and administrative activities. Hence, these networks are dynamic, self-organized, and autoconfigured, allowing nodes to move arbitrarily during communication. MANETs also play an essential role in

Industry 4.0. These networks can be extended and integrated with emerging technologies like cloud technologies, IoT, and machine learning techniques to develop smart applications for automating industrial needs [3, 4]. The structure of the MANET is depicted in Figure 1. Implementation of a secure routing protocol by ensuring QoS is a challenging task in the MANET because of its dynamic topology [5–7]. MANET facilitates open communication infrastructure through which any versatile node can easily join the network and participate in data transmission [8]. This open communication infrastructure provokes security breaches in the MANET [9].

Consequently, the secure and reliable routing in such a network is difficult to accomplish. Generally, routing protocols in MANETs are classified into three categories

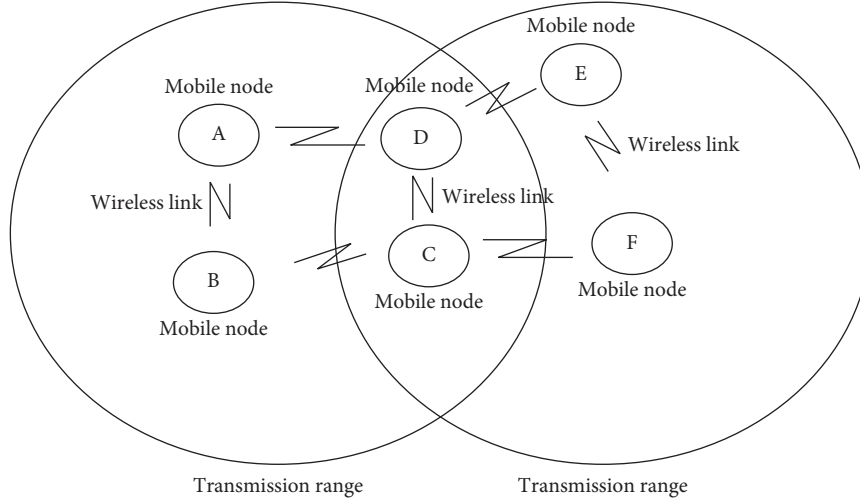


FIGURE 1: Structure of the MANET.

based on their design and routing process: (i) proactive routing protocols, (ii) reactive routing protocols, and (iii) hybrid routing protocols. The proactive routing protocol establishes and maintains all the routes in a routing table prior to the communication. In this category of routing protocols, route setup and route maintenance tasks are accomplished by periodically exchanging the control packets. Transmission of these control packets for route establishment and maintenance leads to routing overhead in the MANET. These proactive routing protocols are suitable for miniature networks.

Unlike proactive protocols, reactive routing protocols establish routes whenever the nodes require them. This route establishment process reduces the network overhead that occurs due to the periodic exchange of control packets in proactive routing protocols. Reactive protocols can determine an optimal path with low packet delay and network overhead compared to the proactive routing protocols. Furthermore, reactive routing protocols apply to more extensive networks. Another category of routing protocols includes hybrid routing protocols. These protocols combine the benefits of both proactive and reactive routing protocols.

Ad hoc on-demand distance vector routing protocol (AODV) is a predominantly used reactive routing protocol in the MANET. Many researchers introspected AODV's performance by considering multiple factors and also identified various reasons that cause security breaches. This protocol has the following flaws:

- (i) There is no mechanism to handle congestion.
- (ii) The existing protocol does not support multipath routing.
- (iii) It is susceptible to various security attacks [10].
- (iv) It does not have any predefined mechanism to handle packet losses.
- (v) It does not have any mechanisms to ensure QoS.
- (vi) There is absence of power optimization concept.

AODV is highly susceptible to various attacks like black hole attack, wormhole attack, DoS attack, and so on. To resolve these security breaches, it is necessary to upgrade the AODV protocol.

Many researchers have proposed different flavors of AODV protocol to handle the issues mentioned above. But no versions of AODV protocols handle all the issues discussed above together as a single protocol. Therefore, the main objective of this proposed protocol is to provide a secure and efficient routing by reducing the packet losses and thereby enhancing the QoS in the MANET. In this paper, we proposed a TBSMR protocol to perform routing by considering the following factors for intensifying the network's efficiency:

- (i) Routing by handling congestion.
- (ii) Secure routing through trusted nodes.
- (iii) Multipath routing.
- (iv) Packet loss reduction.

In MANET, the fundamental reasons for packet loss are the presence of noxious nodes and lack of sufficient battery power of the nodes [11].

The proposed TBSMR protocol integrates all the properties as mentioned above for enhancing the QoS in the MANET.

2. Related Work

2.1. MANET in Industry 4.0. MANETs are in extensive use for achieving the vision of Industry 4.0. Many smarter applications based on MANETs are popping up in various domains to automate and monitor the activities. Such networks are required especially for disaster situations like earthquake, hurricane, flooding, and cyclone, to transfer emergency information for saving lives and properties. These networks can be formulated when there are lean possibilities of physical communication infrastructure. These networks are required to connect people and relay information in emergency situations as in case of recent

bushfire in Australia. MANET-based real-time applications demand precise time-sensitive data transmission. Also in emergency situations, safe sheltering points and escape routes must be accurately delivered to the people in a timely manner. Many existing routing protocols do not emphasize these constraints. Furthermore, the existing routing techniques are based on low-level parameters like; delay, routing overhead, bandwidth, and so on.

Many researchers have proposed QoI-based source selection schemes to transfer time-sensitive critical information. Arsalaan et al. [12] propounded a low overhead source selection approach and QoIT that explicitly considers the user requirements to determine an optimal source, to allow information exchange in emergency situations, by avoiding bottleneck issue.

Convergence of MANET with IoT enlightens another possibility of research in smart ubiquitous computing where ad hoc network plays a vital role in implementing smart city applications. Smart city applications integrate different types of applications of various domains that require different types of message exchanges. Routing in such applications is a challenging task because of the diversity of nodes and disparate message structures. Intelligent routing techniques are required to meet the challenges of Industry 4.0. Intelligent routing protocols can be developed by using emerging technologies like machine learning, bioinspired optimization algorithms, soft computing, and so on.

3. Existing QoS-Based Routing

AODV is a conspicuously used reactive protocol in MANET. But this protocol exhibits many flaws, which are mentioned in Section 2. To overcome these flaws, many researchers developed many AODV-based routing protocols for intensifying the network's efficiency. This section emphasizes the recent flavors of AODV protocols propounded for enhancing the QoS.

Bhagyalakshmi et al. [13] proposed a Q-AODV protocol to determine a noncongested route based on the queue vacancy parameter. This queue vacancy parameter is used to reduce the number of intermediate nodes participating in the route exposure state, thereby reducing control packets' transmission.

Sarkar et al. [14] proposed an enhanced Ant-AODV protocol for optimal route selection in MANET. This protocol uses the ant colony optimization concept for the selection of optimal routes. In this technique, routing is done by computing the pheromone values of all the available paths. A path having the highest pheromone values will be used for transmitting packets from source to destination.

Jhaji et al. [15] propounded the EMAODV protocol for handling congestion. This protocol makes use of the TTL parameter to avoid the flooding of RREQ packets. This TTL parameter is used for identifying the active nodes for forwarding the packets. Only these active nodes are used for forwarding the packets. Unlike active nodes, the other nodes that do not respond to RREQ packets will be treated as silent nodes and are not involved in routing them.

Subramanian et al. [16] developed trust-based AODV in which packets are sent through trusted nodes. A node whose trust value is greater than the threshold value is treated as a trustworthy node; otherwise, it is considered an untrustworthy node. In this protocol, trust values are determined based on the number of request packets, reply packets, and data packets forwarded by each node.

Zhaoxiao et al. [17] proposed an energy-aware EAODV protocol in which a path with low energy cost and having a larger capacity is selected for data transmission. This protocol uses a priority weight parameter to predict the nodes' lifetime based on the present network traffic.

Table 1 outlines the recent existing protocols along with the properties considered to accomplish QoS routing. In our literature study, we considered recent AODV-based protocols developed to overcome the flaws of AODV protocol and we perceived that many researchers considered only a few specific aspects in extending the AODV protocol for enhancing the efficiency of the network. In the implementation of the proposed system, we considered diverse factors like congestion control, malicious node detection, packet loss reduction, and available battery power of nodes during packet transmission. We contemplated all these factors for implementing the proposed TBSMR protocol through which the QoS can be enhanced.

4. Proposed Methodology

The proposed TBSMR protocol functions in three phases for reliable packet transmissions. The three phases of the TBSMR protocol are as follows:

- (i) Route exposure phase.
- (ii) The malicious node detection phase.
- (iii) Information forwarding phase.

This proposed TBSMR protocol is an amended version of the AODV protocol. TBSMR protocol overcomes the flaws of the AODV protocol. In the TBSMR protocol, malicious nodes are detected at every stage in communication. Moreover, the packet loss reduction mechanism is also used for reliable packet delivery. In this protocol, a spurious RREQ is broadcasted by the source node during the initial route revelation process. This spurious RREQ packet contains a fake destination address and destination sequence number. For this spurious RREQ packet, only a malicious node will respond with the RREP packet by claiming that it is having an optimal route to the destination [18, 19]. In this way, the source node identifies the malicious node based on the invalid RREPs received. After identifying the malicious node, the source node propagates this information to all other nodes so that the malicious node will not be considered for forwarding packets and detached from the network. In this way, malicious node detection and elimination are done at the earlier stages of communication. All the nodes other than the malicious nodes are treated as trusted or trustworthy nodes. Also, during communication, malicious nodes are detected and eliminated by computing the nodes' trust values. If the trust value of a node is less than

TABLE 1: Properties of existing routing protocols.

Protocol	Congestion control	Malicious node detection	Packet loss reduction	Energy-aware routing
Q-AODV	✓	✗	✗	✗
Enhanced Ant-AODV	✓	✗	✗	✗
EMAODV	✓	✗	✗	✗
Trust-based AODV	✗	✓	✓	✗
EAODV	✗	✗	✗	✓

the threshold trust value T_{thresh} , then that particular node is marked as a malicious node. A trust value of a node Y is computed based on the trust opinion of its neighbors. Suppose that node X is a neighbor of node Y . Node X can determine the trust opinion on node Y by using a function $T(X, Y)$, where $T(X, Y)$ is a function of three parameters and it is mathematically expressed as $T(X, Y) = f[P(X, Y), N(X, Y), U(X, Y)]$, where $P(X, Y)$ represents successful packet transmissions from node X to node Y ; $N(X, Y)$ indicates failure packet transmissions from node X to node Y ; $U(X, Y)$ represents uncertainty factor that is initially set to 1. The uncertainty factor of value 1 represents that node X is not certain about the trustworthiness of node Y . Depending on the subsequent successful or failure packet transmissions from node X to node Y , $U(X, Y)$ will be updated [18]. $T(X, Y)$ is an average of three parameters and usually ranges from 0 to 1. The obtained value of $T(X, Y)$ represents node X 's trust opinion on node Y and will be maintained by node X in its routing table as **trust_val** of node Y . For a node to be trusted, its **trust_val** ≥ 0.6 . Every node in a network shares trust values of its neighbor nodes with all other nodes periodically, such that only trusted nodes are involved in information exchange while all the nodes whose **trust_val** < 0.6 will be considered as malicious and eliminated from the network. The trust value of a node is updated based on the number of packets forwarded or discarded by it on behalf of other nodes. This protocol is highly reliable because it supports the transmission of acknowledgment after successful transmission of packets from source to destination. When the destination node receives all the packets from the source node, it sends DR (Data Received) packet to the source node. After receiving the DR packet from the destination node, the source node marks the entire route as trusted through which it has transmitted data packets and received the DR packet successfully. Trust value of a route is expressed as follows: $\text{Trust}(\text{route}) = \text{successful packet transmissions} / \text{total packets transmitted}$.

For a route to be trusted, *Trust (route) value* ≥ 0.6 .

5. Routing by Handling Congestion

This protocol supports the concept of multipath routing. This protocol allows source node to maintain multiple routes to the destination in a cache. These multiple routes are used by the source node on occurrence of congestion or link errors. In this proposed protocol, the destination node is allowed to receive multiple RREQs from the same source node for which the destination node sends multiple RREPs. On receiving multiple RREPs from the destination node, the source node selects the best route based on the number

of hops for forwarding the packets. The alternate route towards destination will be stored in the sender's cache used in the future on the occurrence of congestion or link failure. The storage of an alternate path to the destination in a cache avoids invocation of the route discovery process and avoids overwhelming the selected route with packets. In existing protocols, during the routing process shortest and optimal path is opted for sending all the packets, which may lead to the congestion in the selected optimal route. Hence, unnecessary packet loss will occur, which results in reduced throughput. To address this issue, our proposed protocol is implemented so that whenever a selected optimal route is about to get congested, an immediately alternate path stored in the cache will be used by the sender for forwarding the subsequent packets. In this way, load distribution is done by determining the status of congestion of each route.

In this protocol, every node periodically sends the status of congestion to its neighbor using a QS (Queue Status) field in the HELLO packet. Each node determines the status of its available avg. queue by using the following equation:

$$\begin{aligned}
 \text{Min}_{\text{thresh}} &= 0.25 * \text{Total_Buffer_Size}, \\
 \text{Max}_{\text{thresh}} &= 3 * \text{Min}_{\text{thresh}}, \\
 \text{Avg_queuenew} &= (1 - Wq) * \text{Avg_queueold} \\
 &\quad + \text{Instant_queue} * Wq.
 \end{aligned} \tag{1}$$

Here, Wq is the queue weight and is a constant ($Wq = 0.002$ from RED, Floyd, 1997) and Instant_queue is instantaneous queue size [1].

$$QS = \text{Instant_queue} - \text{Avg_queuenew}. \tag{2}$$

If $\text{Queue_Status} < \text{Minthresh}$ indicates no congestion.

If $\text{Queue_Status} > \text{Minthresh}$ and $\text{Instant_queue} < \text{Minthresh}$ indicates likely to be congested.

If $\text{Instant_queue} > \text{Minthresh}$, indicates congestion.

Based on the above calculations, QS field is set to either 0 or 1. This QS field is set in the HELLO packet and sent periodically by each node to its neighbors. Also, before transmitting a packet, every node checks the status of congestion of neighbor nodes by transmitting special acknowledgment packets.

6. Minimizing Packet Loss

A node may discard packets intentionally or due to lack of sufficient battery power for forwarding the packets. These two cases result in unnecessary packet losses, leading to the degradation of network throughput [20–29].

Case 1. Malicious node intentionally discards the packets. A node is considered as a malicious node if the following conditions are met:

- (i) Number of packets received > number of packets forwarded
- (ii) Number of packets forwarded = 0
- (iii) Number of packets received = number of packets forwarded and change in packet size

In all cases as mentioned above, a node is treated as a malicious node.

Case 2. Another reason for packet loss at a particular node is the lack of available battery power for forwarding the packets. In this protocol, before data transmission, the source node gets the status of its neighbor's available battery power by sending a DREQ packet. After receiving the DREQ packet, the node will send its available power to the source through the DREP packet. A node's available power or energy can be determined as follows:

$\text{Thresh_Pow} = 0.10 * \text{Total_Power}$, where Thresh_Pow represents threshold power and Total_Power is the battery power of node.

If any node's $\text{Avail_Pow} \leq \text{Thresh_Pow}$, then this node will not be selected by the source node for forwarding the packets. In this way, a node with a lower energy level will not be considered for packet forwarding. The source node will select an alternate node with sophisticated energy for data transmission. This process will improve the packet delivery ratio through which the QoS can be enhanced.

For reliable data delivery, this proposed protocol scheme uses the concept of acknowledgment packets. Whenever the source intends to send packets to its neighbor, it sends DREQ packet to its neighbor requesting its neighbor node's status. If the neighbor node is active, it immediately responds with the DREP packet. After receiving the DREP packet, the source node sends its data. After completion of data transmission, the source node expects acknowledgment from the neighbor node. After receiving the data, the neighbor node sends DR packet to the source node. This data transmission process continues till all the packets sent by the source node reach the destination successfully. Finally, one acknowledgment packet is sent to the source from the destination node after receiving all the packets. Once the source gets an acknowledgment from the destination node, it considered the route and the intermediate nodes across the route are trusted, and at the same time, trust values are updated. In this way, the proposed scheme ensures reliable packet transmission by minimizing the packet loss; hence, the throughput of the network can be intensified.

The required step to accomplish data transmission in the proposed TBSMR is shown in Figure 2. In Figure 2, node S is the source node, and it is having a route to the destination node D via intermediate node A. Before sending data packets, the source node first checks the trust value of node A. If node A is a trusted node, it checks node A's status by sending the DREQ packet. On receiving DREQ, if node A is having sufficient power for forwarding the packets and is not

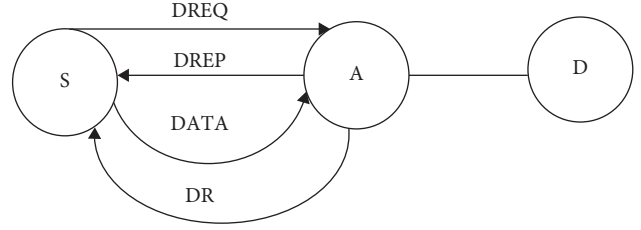


FIGURE 2: Data transmission using TBSMR protocol.

congested, node A will immediately respond with DREP. In this way, packets are transmitted by considering nodes' trust values, congestion status, and sophisticated energy availability.

During packet transmission, a malicious node may repeatedly send DREQ packets to the source node to capture data packets. Whenever a node sends three DREQ packets consecutively, it is marked as a malicious node by the source, and this information is propagated to all other nodes in a network. The algorithm for malicious node detection is explained as follows (Algorithms 1 and 2). where $nrcv$ is the number of received packets, $nfowd$ represents the number of packets forwarded, and $size_of_pkt$ means the packet size.

7. Simulation and Analysis

To analyze the performance of this proposed protocol, we used the NS2 simulation tool. Table 2 represents the parameter considered for simulation in NS2.

The formulation of the MANET by using the proposed protocol is shown in Figure 3. The proposed protocol allows communication between trusted nodes only. To evaluate the performance of the proposed protocol, we considered the metrics like PDR, PLR, average end-to-end delay, and throughput.

7.1. Packet Delivery Ratio (PDR). It is defined as the ratio between the total number of packets received by the total number of packets actually sent.

$$\text{PDR} = \frac{\text{Total no. of packets received}}{\text{Total no of packets sent}} \quad (3)$$

7.2. Packet Loss Ratio (PLR). It represents the number of packets lost during transmission. It is the ratio between the total number of packets lost by the total number of packets received.

$$\text{PLR} = \frac{\text{Total no. of packets lost}}{\text{Total no. of packets received}} \quad (4)$$

7.3. Average End-to-End Delay. It is defined as an average time taken by packets to reach from source to destination; this includes transfer time, propagation delay, queuing time, and processing time.

```

Step 1: Intiate_DummyTransact ( )
{
  Step 1.1: Source Node broadcasts Dummy RREQ with fake Destination Address and
  Destination Sequence Number using Send_Dummy_RREQ ( ) function.
  Step 1.2: if (RREP == received)
  Mark corresponding node as Malicious Node.
  Propagate this malicious node ID to other nodes in a network.
}

Step 2: Route Discovery Initiated by Source Node.
Step 3: Route Establishment by considering trust values of nodes.
Step 4: Packet Transmission from Source Node to Destination
for each node on the existing route do
  Check Trust value (trust_val), Congestion status and Available energy level
  If ((trust_val>0.6) andand (QS==0) andand (Avail_Pow > Thresh_Pow))
  {
    Send DREQ to the next node in routing table and wait for DREP
  }
  if (DREP == received)
  Send data packets to the next node and wait for DR (Data Received) packet
  if (DR == received)
  Mark node as trusted.
  Update and propagate trust value of node.
}

  else if ((trust_val>0.6)
  {
    if ((QS == 1) || (Avail_Pow ≤ Thresh_energy))
  {
    Select Alternate route from cache for forwarding the packets.
    goto Step 4.
  }
  else if (trust_val<0.6)
  {
    Marks node as malicious and remove from the routing table.
    Select alternate route if available, Otherwise
    goto Step 2.
  }
  else
  re-establish route using step 2 and repeat the process.
}

```

ALGORITHM 1: Routing process.

```

Malicious_node_detection ( )
{
  for each neighbor node n
  do
    if (nrecv > nfowd) || (nfowd == 0)
    {
      mark node n as malicious. propagate this information to other nodes
    }
    else if (nrecv == nfowd)
    {
      If (size_of_pkt! = 512 bytes)//change in packet size
      {
        Mark node n as malicious node
        Propagate this information to other nodes
      }
    }
    else
    forward packets to node n
  }
}

```

ALGORITHM 2: Malicious node detection.

TABLE 2: Simulation parameter.

Parameter	Values
Coverage area	500 m \times 500 m
Simulation time	500 sec
No. of nodes	50, 100 and 300
Traffic type	UDP-CBR
Transmission range	250 m
Packet size	512bytes
Maximum speed	20 m/s
Routing protocol	TBSMR
Mobility model	Random way point

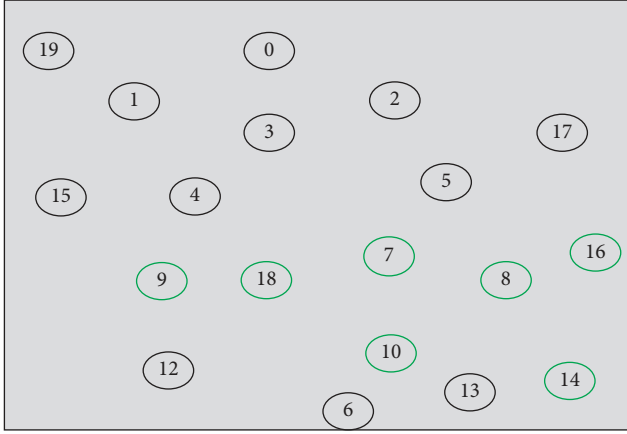


FIGURE 3: Formulation of MANET.

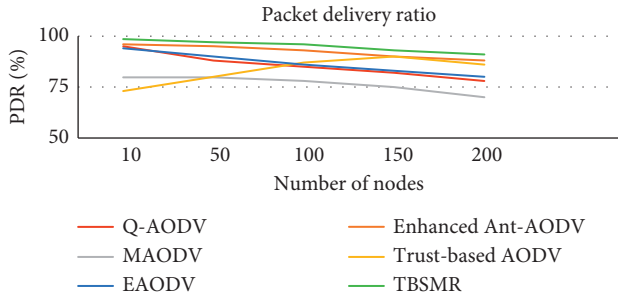


FIGURE 4: Comparison of PDR.

7.4. Throughput. It is the rate at which destination receives data in bits per unit time in the network. It is expressed in kbps.

Figure 4 shows that the proposed TBSMR protocol exhibits better PDR than the existing approaches.

Figure 5 illustrates that the proposed TBSMR protocol has less packet loss ratio than the existing routing techniques.

Figure 6 justifies that the proposed routing technique exhibits a lower average end-to-end delay in comparison with the other existing routing schemes.

The proposed TBSMR protocol has better throughput than the existing routing approaches considered in this study, and the same is depicted in figure 7.

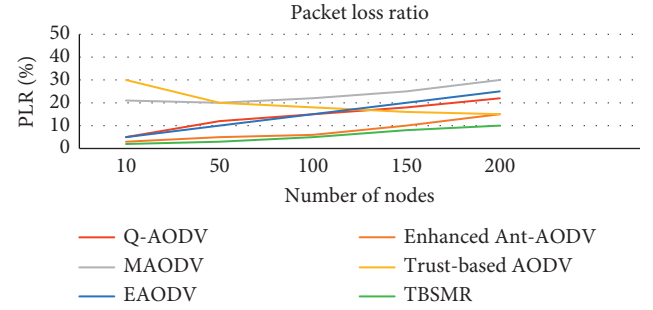


FIGURE 5: Comparison of PLR.

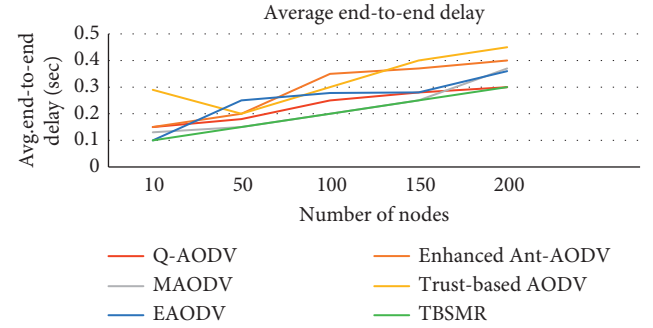


FIGURE 6: Comparison of average end-to-end delay.

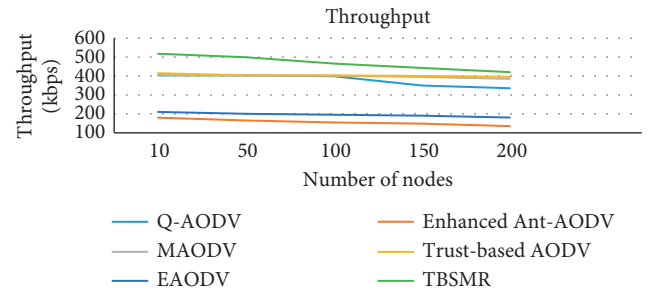


FIGURE 7: Comparison of throughput.

Table 3 demonstrates precisely that the proposed routing technique outperforms by considering multifactors to intensify the QoS in the MANET.

TABLE 3: Performance comparison of the existing and proposed protocol.

Routing protocols	Congestion handling	Data loss level (%)	PDR (%)	Malicious node detection	Multipath routing	Throughput
Q-AODV	Yes	19	79	No	No	Moderate
Enhanced Ant-AODV	Yes	18	96	No	No	Low
EMAODV	Yes	20	80	No	Yes	Moderate
Trust-based AODV	No	18	91	Yes	No	High
EAODV	No	16	90	No	No	Low
Proposed method	Yes	10	98	Yes	Yes	High

All the simulated results justify that the proposed routing protocol exhibits better performance than the existing approaches in enhancing the QoS and making it suitable for real-time applications.

8. Conclusion

In this work, we proposed a routing protocol called TBSMR to enhance the QoS of the MANET. It is applicable for more extensive networks and considers multifactors like congestion, trust values of the nodes, and the available battery power of nodes during the routing process, which results in better performance with reduced overhead. Moreover, this proposed protocol supports multipath routing that minimizes the floating of unnecessary control packets for route establishment in congestion or node failure. This protocol also ensures secure communication by detecting malicious nodes. Our simulation results justify that the proposed TBSMR protocol gives better performance in PDR, PLR, average end-to-end delay, and throughput compared to the existing routing techniques. Overall, this proposed TBSMR routing approach enhances the QoS of the MANET besides ensuring secure communication.

In the future, we emphasize the implementation of security algorithms by incorporating encryption, decryption, and blockchain approaches for providing high security to the MANET.

Data Availability

Access to all the supporting data about this article will be given based on the requests directed through the data access committee and institutional review board.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] M. D. Sirajuddin, C. Rupa, and A. Prasad, "Advanced Congestion Control Techniques for MANET," *Advances in Intelligent Systems and Computing*, vol. 433, pp. 271–279, 2016.
- [2] L. Femila and M. Marsaline Beno, "Optimizing transmission power and energy efficient routing protocol in MANETs," *Wireless Personal Communications*, vol. 106, no. 3, pp. 1041–1056, 2019.
- [3] B. Chen, J. Wan, L. Shu, L. Peng, M. Mukherjee, and B. Yin, "Smart factory of Industry 4.0: key technologies, application case, and challenges," *Institute of Electrical and Electronics Engineers Access*, vol. 6, 2018.
- [4] H. Kathiriya, A. Pandya, V. Dubay, and A. Bavarva, "State of art: energy efficient protocols for self-powered wireless sensor network in IIoT to support industry 4.0," in *Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1311–1314, Noida, India, June 2020.
- [5] T. Li, J. Ma, and C. Sun, "SRDPV: secure route discovery and privacy-preserving verification in MANETs," *Wireless Networks*, vol. 25, no. 4, pp. 1731–1747, 2019.
- [6] T. Singh, J. Singh, and S. Sharma, "Survey of secure routing protocols in MANET," *International Journal of Mobile Network Design and Innovation*, vol. 6, no. 3, pp. 142–155, 2016.
- [7] S. Hossain, M. S. Hussain, R. R. Ema, S. Dutta, S. Sarkar, and T. Islam, "Detecting Black hole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET," in *Proceedings of the ICCCN*, pp. 1–7, Kanpur, India, June 2019.
- [8] V. V. Sarbhukan and L. Ragha, "establishing secure routing path using trust to enhance security in MANET," *Wireless Personal Communications*, vol. 110, no. 1, pp. 245–255, 2020.
- [9] H. Moudni, M. Er-routidi, H. Mouncif, and B. El Hadadi, "Secure routing protocols for mobile ad hoc networks," in *Proceedings of the IT4OD*, pp. 1–7, Fez, Morocco, March 2016.
- [10] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in *Proceedings of the JEEIT*, pp. 28–33, Amman, Jordan, April 2019.
- [11] N. Sarmah, Y. Yang, H. Sharif, and Y. Qian, "Performance analysis of MANET routing protocols by varying mobility, speed and network load," in *Proceedings of the ICSPCS*, pp. 1–6, Cairns, Australia, March 2015.
- [12] A. ShakaybArsalaan and H. Nguyen, "Andrew coyle and MahrukhFida, " quality of information with minimum requirements for emergency communications," *Adhoc Networks*, vol. 111, pp. 1570–8705.
- [13] Bhagyalakshmi and A. K. Dogra, "QAODV: A flood control ad-hoc on demand distance vector routing protocol," in *Proceedings of the ICSCCC*, pp. 294–299, Jalandhar, India, March 2018.
- [14] D. Sarkar, S. Choudhury, and A. Majumder, "Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network," *Journal of King Saud University-Computer and Information Sciences*, vol. 8, 2018.
- [15] H. Jhaji, R. Datla, and N. Wang, "Design and implementation of an efficient multipath AODV routing algorithm for MANETs," in *Proceedings of the CCWC*, pp. 0527–0531, Las Vegas, NV, USA, December 2019.
- [16] S. Subramanian and B. Ramachandran, "Trusted AODV for trustworthy routing in MANET," *Advances in Intelligent Systems and Computing*, vol. 167, pp. 37–45, 2012.
- [17] Z. Zhaoxiao, P. Tingrui, and Z. Wenli, "Modified energy-aware AODV routing for ad hoc networks," *WRI Global Congress on Intelligent Systems*, pp. 338–342, 2009.

- [18] M. S. Hussain and K. U. R. Khan, "Network-based anomaly intrusion detection system in MANETS," in *Proceedings of the ICISC*, pp. 881–886, Coimbatore, India, December 2020.
- [19] M. Sirajuddin, C. Rupa, and A. Prasad, "A trusted model using improved-AODV in MANETS with packet loss reduction mechanism," *Advances in Modelling and Analysis B*, vol. 61, no. 1, pp. 15–22, 2018.
- [20] M. D. Sirajuddin, C. Rupa, and A. Prasad, "An innovative security model to handle blackhole attack in MANET," *Proceedings of International Conference on Computational Intelligence and Data Engineering*, vol. 9, pp. 173–179, 2018.
- [21] G. Rathee, S. Garg, G. Kaddoum, D. N. K. Jayakody, M. J. Piran, and G. Muhammad, "A Trusted Social Network Using Hypothetical Mathematical Model and Decision- Based Scheme," *Institute of Electrical and Electronics Engineers Access*, vol. 9, pp. 4223–4232, 2021.
- [22] H. Lin, J. Hu, W. Xiaoding, M. F. Alhamid, and M. J. Piran, "Towards secure data fusion in industrial IoT using transfer learning," *Institute of Electrical and Electronics Engineers Transactions on Industrial Informatics*, vol. 20201, page, 2020.
- [23] S. Venkatraman and M. Alazab, "Use of data visualisation for zero-day malware detection," *Security and Communication Networks*, vol. 2018, 2018.
- [24] D. Vasan, M. Alazab, S. Wassan, H. Naeem, B. Safaei, and Q. Zheng, "IMCFN: image-based malware classification using fine-tuned convolutional neural network architecture," *Computer Networks*, vol. 171, Article ID 107138, 2020.
- [25] Q. V. Pham, K. Dev, P. K. R. Maddikunta, T. R. Gadekallu, and T. Huynh-The, "Fusion of federated learning and industrial internet of things: a survey," 2021, <https://arxiv.org/pdf/2101.00798.pdf>.
- [26] S. Rajadurai, M. Alazab, N. Kumar, and T. R. Gadekallu, "Latency evaluation of SDFGs on heterogeneous processors using timed automata," *Institute of Electrical and Electronics Engineers Access*, vol. 8, pp. 140171–140180, 2020.
- [27] C. O. Iwendi and A. R. Allen, "Enhanced security technique for wireless sensor network nodes," in *Proceedings of the IET Conference on Wireless Sensor Systems (WSS 2012)*, pp. 1–5, London, UK, June 2012.
- [28] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, "The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems," *Sensors*, vol. 20, no. 9, Article ID 2559, 2020.
- [29] M. Mittal, C. Iwendi, S. Khan, and J. A. Rehman, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system," *Transactions on Emerging Telecommunications Technologies*, Article ID e3997, 2021.