International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212331 Volume 9, Issue 2, March – April (2022)

RESEARCH ARTICLE

RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET

P.T. Kasthuri Bai
Department of Computer Science, Thiruthangal Nadar college, Chennai, Tamil Nadu, India
thulasingamkasthuri2016@gmail.com

Received: 31 December 2021 / Revised: 26 February 2022 / Accepted: 02 March 2022 / Published: 30 April 2022

Abstract – In recent years, the Internet of Things (IoT) has become the most innovative and efficient technology globally. IoT uses physical devices for establishing a real-time interconnection between heterogeneous networks. MANET plays an essential role in IoT-based systems for multi-hop data transmission, rapid setup, dynamic topology, etc. Generally, MANET is structureless and does not require any base station to achieve data transmission. In MANET, routing plays an important role, and modern IoT devices' evolution supports routing efficiency. MANET with IoT is applicable for various applications like emergency operations, disaster management, and environmental monitoring. Several mechanisms evolved to achieve secure routing on MANET with IoT. But still, achieving enhanced MANET performance with satisfying all QoS parameters is a challenge. Most of the existing systems lack a secured routing system, and there is no proper predefined mechanism for handling the packet losses. However, few approaches support multipath routing but fail to obtain the optimal power consumption. We use the routing manager-based secure rate analysis (RMBSRA) mechanism to address these issues. The proposed system is a centralized mechanism built with three major components: routing manager, neighboring table, and routing table. These components are responsible for effective packet transmission in the shortest path without data losses. The proposed system improves the multicast routing system by balancing the bandwidth allocation and eventually traffic on the network. The proposed RMBSRA performance is evaluated in the simulation environment NS-2. The observation obtained from RMBSRA is compared with the existing Trust-Based Secure Multipath Routing Protocol (TBSMR) and real-time secure route analysis (RSRA). The proposed RMBSRA achieves enhanced routing performance compared to the existing mechanisms.

Index Terms – IoT, MANET, Routing Protocol, Security, Load Balancing, Traffic, Multipath Routing.

1. INTRODUCTION

Wireless technology enables enhanced flexibility in networking and allows users to access their data remotely. Nodes are wirelessly connected in ad-hoc networks without the need for administration or infrastructure assistance. The Internet of Items (IoT) is a cutting-edge technology that allows things to interact globally through networks and communication technologies. The more connected machines, the more data is generated, and hence the more routing traffic is generated. The collaboration between MANET and the Internet of Things (IoT) reopens new channels for service demand in smart surroundings [1 - 5].

1.1. IoT

Kevin Ashton coined the term "internet of things" in 1999, and initially, it was known as "internet for things," which was later shortened to "Internet of Things." It was first discussed in 1982 as an idea of a network of smart devices as a modification of a Coke machine that was cold when freshly filled cokes were loaded [6,7]. The Internet of Things (IoT) is a technology that allows physical objects to communicate digitally. The internet of people revolutionized the world, but a new internet is emerging that is focused on linking things, hence the name "internet of things" (IoT), where objects exchange their experiences and communicate with one another. The internet of things is interconnected via the internet of computing devices embedded in everyday objects, enabling all of them to join together for transmitting and receiving data, just like the internet is a means or way to connect individuals who are separated by a great distance.

1.2. MANET

MANET contains various connected nodes independent of moving anywhere in direction and speed. MANET topology is dynamic, which affects the different QoS performances. To enable reliability on internet-based services, MANET is evolved, making the user access the application independently. Commonly mobile nodes' connection and transmission are within the radio frequency range. This restriction on transmission range affects the node's communication directly from the source to the destination node. As a result, it leads to cooperative transmission. Initially, the source node chooses the route and moves the

RESEARCH ARTICLE

packets to the intermediate nodes; the same procedure follows until the packet reaches the destination node. Similar to other networks, MANET also suffers from numerous attacks and threats challenges [8,9]. The malicious nodes capture the packets transmitted through intermediate nodes and enable multiple attacks like a sinkhole, Modification, Eavesdrop, and more. These threats need to be overcome to achieve reliable network performance.

1.3. MANET-IoT Systems

Internet of Things (IoT) has become one of the top emerging domains in recent years, and it has an impact on device controlling and device assessing remotely. It is similar to the working of sensor noes. In the modern world, numerous IoT devices are introduced for supporting various activities. As a result, most researchers suggest IoT as a prominent for executing efficient routing. But it has the maximum possibility of severe threats like Blackhole attacks, wormhole attacks, Distributed DoS attacks, pantomime, Byzantine attacks, etc. This research focused on establishing a secure routing, and it continues in delivering enhanced strategic methods for MANET.

Quality of service (QoS) is dependent upon different network parameters. If routing performance is maximized means automatically throughput is also enhanced. Throughput maximization results in a decrease in packet drop ratio and delay. Another significant impact of an efficient route is better retransmission frequency because inefficient routes maximize retransmission frequency. Lack of retransmission frequency affects throughput performance and delay ratio.

In MANET, routing is the whole responsibility for achieving efficient throughput performance. Routing can be executed in various ways; its difference is based on the parameters taken for route selection. The routing path count and characters differ based on the number of hops, IoT devices, mobility, energy, etc. The main aim of these route discoveries is to achieve enhanced and secure routing [10-12]. The routing on IoT devices has maximum possibility of security threats. Here the route discovered is untrusted as it belongs to some other; hence the IoT device trustworthiness needs to be confirmed on execution.

To address the existing issues, we proposed Routing manager-based secure rate analysis (RMBSRA) mechanism, and the main contribution of this work are listed below;

- Implementation of the multipath routing system
- It overcomes the drawback of an existing multipath routing protocol such as network traffic and bandwidth allocation.
- The system considers the sleeping node.
- Implementation of the centralized routing management system
- Effective in identifying available routing paths

The organization of the work is as follows: In section 1 introduction is described, related work is discussed in section 2, proposed work is described in section 3, section 4 contains the result and discussion, and finally, section 5 contains the conclusion part.

2. RELATED WORK

There are various mechanisms evolved for establishing a secure routing system. In this section, different MANET methods are discussed in detail.

Mohammed Hussain et al. [13] proposed a Network-based Anomaly Intrusion Detection System for MANET. The existing system is suffered from unique vulnerabilities and unsafe characteristics of the same solution. High energy consumption is the primary issue, and it is addressed using a combined intrusion detection mechanism for enhancing the MANET protections. The main goal of this proposed system is to detect the anomalous node's behavior in terms of working battery life or energy. However, it is applicable for minimum workload, but in the case of vast and dynamic workloads, there is no defined structure for handling the workloads and the security.

Hui Lin et al. [14] proposed an IoT transfer learning mechanism to establish a secure data fusion. The main reason for the proposed system is to address the need for multiple training learning models for data analysis which results in the lack of meeting real-time requirements in IIoT. To overcome this, the proposed TDF is built with three major components such as classification using Guidance-based Deep Deterministic Policy Gradient (GDDPG) system, privacy preservation using the multi-blockchain mechanism, and grouping task receivers using transfer learning-based GDDPG. The TSDF result in low latency high throughput with enhanced security in data fusion for IoT applications. But there is no detail about controlling the network traffic and data losses.

Sivashankari Rajadurai et al. [15] proposed the implementation of Timed Automata for latency evaluation of Synchronous Data Flow (SDF) in a graphical model. Latency is significant in multimedia processing applications as exceeding threshold results in poor service quality (QoS). The proposed system includes the timed automata used on the heterogeneous multiprocessor platform to achieve this. The timed automata represent the system model, containing an execution platform and synchronous data flow. However, this approach fails to e latency consider other constraints like buffer size and energy consumption.

RESEARCH ARTICLE

Mohammad Sirajuddin et al. [16] proposed Trust-Based Secure Multipath Routing Protocol (TBSMR) for improvising the MANET QoS's. Achieving safe and energy-efficient data transmission in MANET is a difficult task. The main advantage of the proposed model includes various QoS factors like secured data transmission, packet loss reduction, congestion control, and malicious node detection. The proposed model achieves secure and energy-efficient data transmission by considering these factors. But this mechanism is failed to handle the routing congestion.

P. Sathyaraj et al. [17] proposed a trust‑based performance evaluation method for designing a secured protocol for IoT devices in MANET. It is a real-time secure route analysis (RSRA) method for implementing secure routing in MANET. It provides the route list from source to destination nodes. The trustworthiness of the IoT devices is measured by mobile node fast route support (MSRS) and device support (DS). Data forwarding support (DFS) of the routes is measured using these two factors. The DFS factor determines the selected route, which achieves the QoS of MANET. The major drawback of this system is the absence of a power optimization concept.

Swetha et al. [18] discussed the major MANET issue is preserving the node safe so that it cannot be easily detected while routing. For this, the author developed a secured, robust, location-oriented routing method (S2MLBR), in which the network is divided into several regions using mysterious locations. In each region, the trustworthiness of each node is calculated by the signal strength, cooperation rate, mobility, and link failure. Insecure routing, the trust model is executed to calculate various routes' trustworthiness. But it results in path loss and minimum cooperation rate in the network.

Belgaum et al. [19] proposed that in mobile ad hoc networks, routing methods are used to send packets from the source to the destination node. Intruders look for opportunities to break into the network, leading to network failure. The existing protocols are vulnerable to attacks at all times, for the author proposed a reactive secure routing method using the triple factor. It measures the node's trust using direct details and indirect reputation from neighbor nodes. The proposed method estimates the trustworthiness of the route selection. But this approach is suffered from overload or scarcity of the system resources.

Guaya-Delgado et al. [20] address the issue of non-cooperation among the nodes in the network. The amount of delivered packets is substantially reduced when selfish nodes refuse to collaborate in this execution. To overcome this, a reputation-orient routing method is proposed for improving MANET security. In the network, the neighbor node measured the reputation of another node locally and based on the node's reputation; the route selection process was performed. But in this mechanism, the performance of accurate estimation on the path is not significant.

Mukhedkar et al. [21] proposed implementing a hybrid optimization algorithm for developing a trust-based secure routing system. The existing approaches do not, or lack is designing a definite cooperative and trustworthy system. The Dolphin Cat Optimizer analyzes the trust factor and executes the route selection. The trust factor is interpreted in two ways: current and historical values. The trust analysis is performed directly and indirectly according to the node delay, distance, and lifetime. However, the absence of a centralized monitor system makes this approach less effective.

Veeraiah and Krishna et al. [22] proposed MANET's novel secure multipath routing mechanism. The main focus of this approach is to enhance the performance metrics on the aspect of packet delivery ratio and security. The proposed system is a clustering mechanism that uses fuzzy clustering for performing nodes cluster and cluster head selection based on the energy level. The nodes classification is done using the naïve Bayes classifier. The optimal route selection is based on major factors like throughput, connectivity, trust, and energy. But this approach does not deal with multiple shortest paths, and there is no statement about the sleeping or inactive nodes and controlling maximum energy consumption.

Singh, K., & Gupta, R et al. [23] proposed a new ad-hoc routing protocol known as SO-AODV (Secured and Optimized Ad-Hoc On-Demand Distance Vector). The main intention of proposing this mechanism is to enable an effective communication system during disaster situations. In which pigeons swarm optimization (PSO) is applied for selecting the shortest path with a minimum hop count. For enabling security, the ciphertext stealing technique (CST) is implemented with qu-Vanstone elliptic curve cryptography (Vq-ECC) based public-key cryptography system. But this mechanism has no detailed report about energy consumption and how it is optimized throughout the packet transmission.

Along with the among existing systems, various research works evolved in the motto of establishing an effective multicast routing system [24 - 27]. However, the need for a prominent mechanism is still in the development stage. The dynamic topology makes implementing a safe routing protocol and preserving QoS a difficult task in the MANET [28-32]. The above-mentioned existing system's advantage and their effort on fulfilling the MANET need motivate the states the need of proposing a centralized multicast routing system using balancing the bandwidth allocation and traffic eventually on the network

2.1. Problem Statement

- Existing methods fail to achieve QoS factors in MANET.

RESEARCH ARTICLE

- There is no clear consideration about whether the sleeping node will affect the network performance in the existing system.
- Most of the existing systems describe the single routing system.
- Lack of centralized monitoring system.
- Lack of tracking the nodes past and current activities in the network

3. PROPOSED ROUTING MANAGER-BASED SECURE RATE ANALYSIS (RMBSRA)

3.1. RMBSRA Workflow

Figure 1 illustrates the proposed mechanism which implements multipath routing for providing multiple routes from source to destination nodes. The main advantage of multipath routing is that it ensures the packet delivered successfully even on link failures. If link failure occurs, it chooses the following alternative available path for successful execution. The multipath routing system has three major components: route discovery, traffic allocation, and route maintenance. Multipath routing effectively handles the load balancing by distributing the traffic towards the multiple routes. Multipath routing systems can be discovered quickly and also provide packet reordering. The significant disadvantages of Multipath routing protocols are complexity and overhead. The quality of traffic is significant in traffic allocation. This paper proposes routing manager-based secure rate analysis (RMBSRA). RMBSRA balances the traffic and bandwidth allocation to enhance the multicast routing system's overall performance. Multiple works initiated in improving the routing but lack detail on describing the sleeping node effect on network performance. The main advantages of the proposed system are listed below;

- Implementation of Routing Manager
- Implementation of Neighboring Table
- Implementation of Routing Table

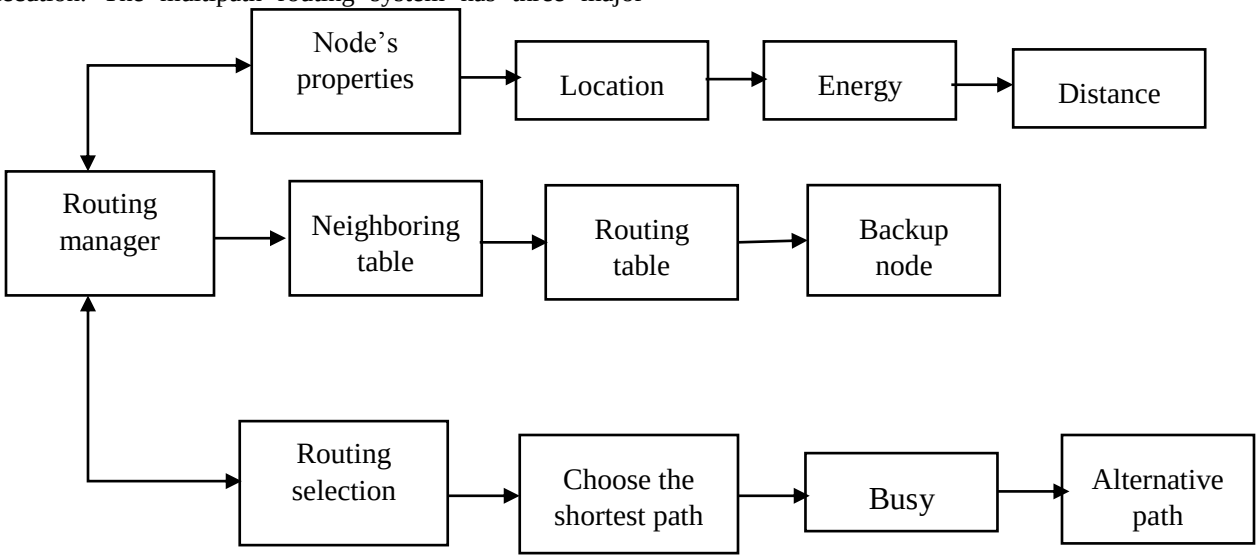

Figure 1 Proposed Architecture

3.2. Routing Manager (RM)

The routing manager (RM) plays a vital role in the proposed system. The node with the highest energy level in the network is selected as the Routing Manager. The RM is responsible for creating a backup node or equivalent node (BU). It acts as the next RM in case the energy level of the current RM gets drained.

3.3. Neighboring Table

The routing manager handles the neighboring table, which controls all nodes' activities like distance, energy, speed, and location. The major components in the proposed system are Routing Manager, Route Planning, and the network model. The proposed execution starts with the network deployment with nodes in the range of 1800*1800 network area. In the proposed RMBSRA, the routing manager is the essential component responsible for the entire network performance. After the network deployment is done, all the nodes in the network are registered. The algorithm flow covered entire proposed mechanism in algorithm 1; after that identification process begins by confirming which nodes are inactive states and which nodes are in sleeping or idle state in the network. The inactive state nodes are qualified for taking part in packet communication. Once the sleeping node's status is changed

RESEARCH ARTICLE

into an active state, it will also take part in packet transmissions. The RM observes the node's position deeply and updates in the neighboring table as described in figure 2. The neighboring table contains all node activity details and regularly updates the inactive and cooperative node lists. The inactive states' nodes are categorized under the cooperative node list, and the nodes in idle or sleeping states are categorized under the inactive node list. Using the neighboring table information, the RM systematizes the nodes ready to participate in network transmission.

Node ID	Location	Speed	Distance	Energy

Figure 2 Neighboring Table Structure

Begin

{

Initialize the mobile nodes randomly manner (1800*1800) network size;

Elect the routing manager (RM) backup node (BU);

RM → highest energy ∗ higest bandwidth(memory)[BU]

Allocate the highest energy and a memory allocation (RM);

Secondary which node act as backup node (BU);

Neighboring node properties;

i) Mobile node distance $M_{i,j}$, (d)

ii) Mobile node speed $M_{i,j}$, (s)

iii) Mobile node energy $M_{i,j}$, (e)

iv) Mobile node bandwidth, $M_{i,j}$, (BW)

2) $M_{i,j}, (d) = \sqrt{(a_{i1} - a_{j1})^2 + (b_{i2} - b_{j2})^2}$

The above expression calculates the node's distances in which a and b are the coordinate positions.

3) $M_{i,j}, (s) = M_{i,}(\text{sequence no}), \text{set\_d}_{st}(x_{path}, y_{path}, n_{speed})$

Where the x and y are the position path and n determine the nodes speed

4) $M_{i,j}, (e) = \left(\frac{E_{ix} - R_{ix}}{c_t}\right)$

Where E_{ix} → initial energy;

R_{ix} → Residual Energy;

c_t → communication cost

5) $M_{i,j}, (bw) = \left(\frac{N_{pkt}(tx) * S_{pkt}}{T_t}\right)$

The size of the packet transmitted and the total time taken calculated the total consumed bandwidth. Where $N_{pkt}(tx)$ → the number of packets transmitted; S_{pkt} → size of the packet; T_t → total time taken to transmit

RM → $M_{i,j}, (d), M_{i,j}, (e), M_{i,j}, (s), M_{i,j}, (BW)$ // updated to routing manager

}

Algorithm 1 Routing Manager Based Secure Rate Analysis

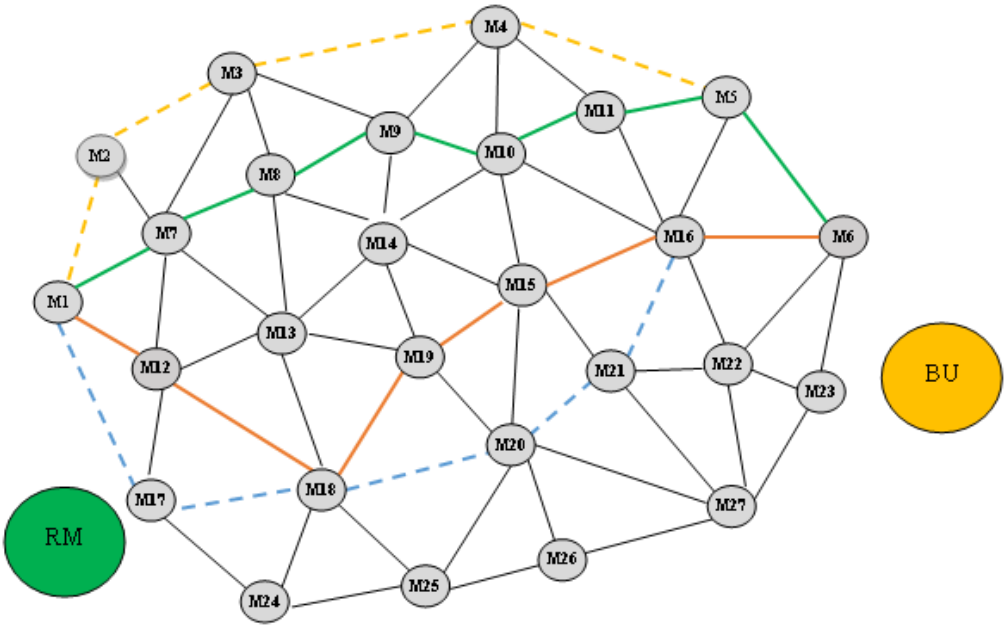

Figure 3 Proposed Routing Structure

RESEARCH ARTICLE

3.4. Routing Table

The routing table describes the RM node with the highest bandwidth in the network. The nodes with the next energy level to the RM node are elected as the secondary node BU. Figure 3 describes the proposed architecture in which the total mobile nodes are deployed between M1 – M21. Multiple paths are available between these nodes, and the routes are arranged in the neighboring node table. The route selection is categorized into the current, upcoming, and alternative routes based on the nodes' distance, speed, energy, and bandwidth is clearly explaining algorithm 1. The available routes are described in the table 1.

Table 1 Routing Details

Route No	Current Route	Upcoming Route	Alternative Route
1	M1-M7-M8-M9-M10-M11-M5-M6	M1-M12-M18-M20-M21-M16-M6	M1-M17-M18-M20-M21-M16-M6
2	M1-M12-M18-M20-M21-M16-M6	M1-M7-M8-M9-M10-M11-M5-M6	M1-M2-M3-M4-M5-M6
3	M1-M7-M8-M9-M10-M11-M5-M6	M1-M2-M3-M4-M5-M6	M1-M12-M18-M20-M21-M16-M6

Table 1 describes the available routes in three categories: current, upcoming, and alternative routes. The currently available route is M1-M7-M8-M9-M10-M11-M5-M6, and the following upcoming route to the current route is M1-M12-M18-M20-M21-M16-M6, and the alternative route is M1-M17-M18-M20-M21-M16-M6. If the current route fails or is drained, then the upcoming route becomes the current route M1-M12-M18-M20-M21-M16-M6, the alternative route becomes the next upcoming route M1-M7-M8-M9-M10-M11-M5-M6, and another new alternative route is created, such as M1-M2-M3-M4-M5-M6. Then again, the upcoming route M1-M7-M8-M9-M10-M11-M5-M6 becomes the current node, the next available route M1-M2-M3-M4-M5-M6 becomes the upcoming route, and another new route, M1-M12-M18-M20-M21-M16-M6, is discovered. This routing cycle will continue by creating new routes till the packet successfully reaches the destination.

4. EXPERIMENTAL RESULTS

4.1. Simulation Environment and Parameters

The proposed Routing manager-based secure rate analysis (RMBSRA) performance is examined in NS-2. NS-2 is the network Simulator-2, a popularly known simulation setting used for execution among research scholars. In this experimental setup, the network is deployed dynamically in the range of 1700 × 1700 $m^{2.}$ The total number of nodes deployed in the network is 120 using the dynamic model. According to which the nodes are independent of moving anywhere within the range. The Random way mobility model is taken for executing the dynamic model. The 802.11 Mac protocol is the link-layer protocol with IEEE standard is used in this work. Next, the network traffic is created using the multicast constant bit ratio. The IEEE 802.11e and 802.11b are the heterogeneous and WLAN traffic taken for analysis. Using the TCP or UDP network topology data connection is established. The packet size used for the transmission is 2000 bytes with the mobility range of 10-35/ms, and the packets travel 24 Mbps data rate. In the experiments, other parameters used are explained in below table 2.

Table 2 Simulation Parameters and its Values

Simulation Parameter	Value
Simulator	NS-2
Simulation time	200 s
Number of nodes	120
Simulation area	1700 × 1700 m^2
Mac Protocol	IEEE 802.11
Data rate	24 Mbps
Radio range	100m
Mobility model	Random waypoint model
Antenna	Omnidirectional antenna
Node speed	10-35 m/s
Packet size	512 bytes
Traffic type	Multicast constant bit ratio

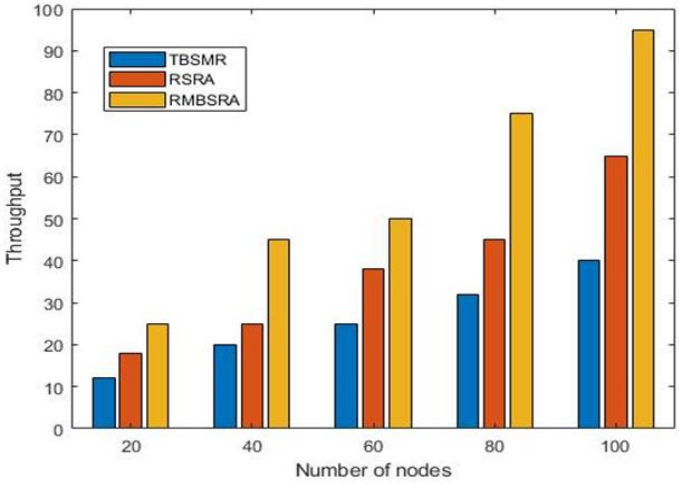

Figure 4: Throughput Vs. number of nodes

RESEARCH ARTICLE

The figure 4 describes the performance comparison between the proposed Routing manager based secure rate analysis (RMBSRA) with Trust-Based Secure Multipath Routing Protocol (TBSMR) and real-time secure route analysis (RSRA). The evaluation metric discussed here is throughput, and it is calculated through a number of nodes involved with its achieved throughput. The x-axis shows the total nodes taking part in an experiment in which the node count is raised by 20 at regular intervals. The Y-axis shows the total throughput attained by respective nodes. The proposed RMBSRA achieves 25% of throughput for 20 nodes, 45% of throughput for 40 nodes, 55% of throughput for 60 nodes, 75% of throughput for 80 nodes, and 97% for 100 nodes. At the same time, the RSRA achieves 17% of throughput for 20 nodes, 24% of throughput for 40 nodes, 37% of throughput for 60 nodes, 42% of throughput for 80 nodes, and 68% of throughput for 100 nodes. And the TBSMR achieves 11% of throughput for 20 nodes, 18% of throughput for 40 nodes, 26% of throughput for 60 nodes, 32% of throughput for 80 nodes, and 38% of throughput for 100 nodes. The throughput performance attained by RMBSRA is more efficient than the others.

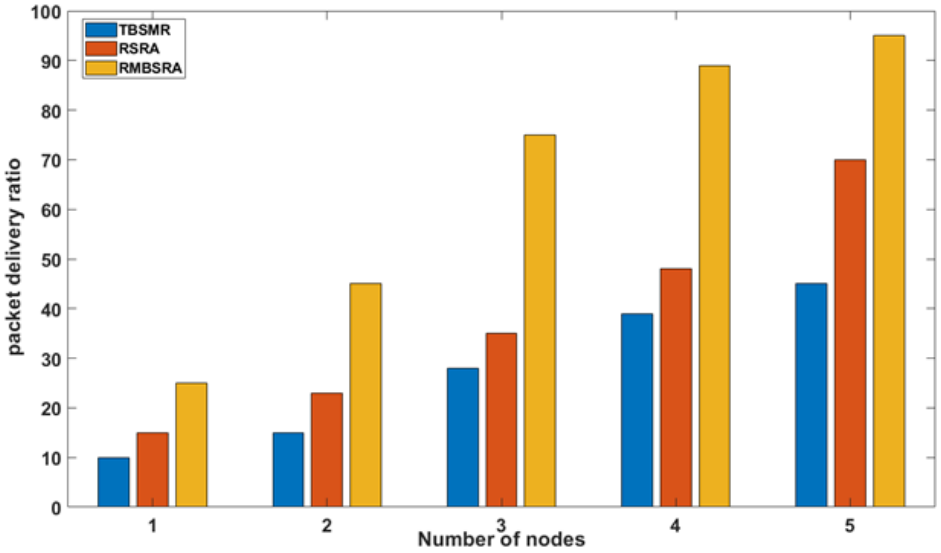

Figure 5 Packet Delivery Ratio (PDR) Vs. the Number of Nodes

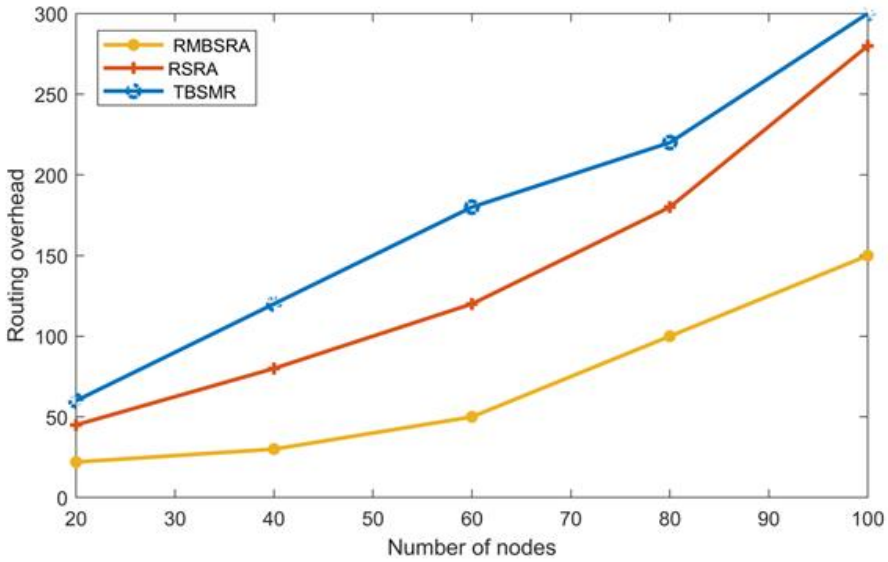

Figure 6 Routing Overhead Vs. Number of Nodes

RESEARCH ARTICLE

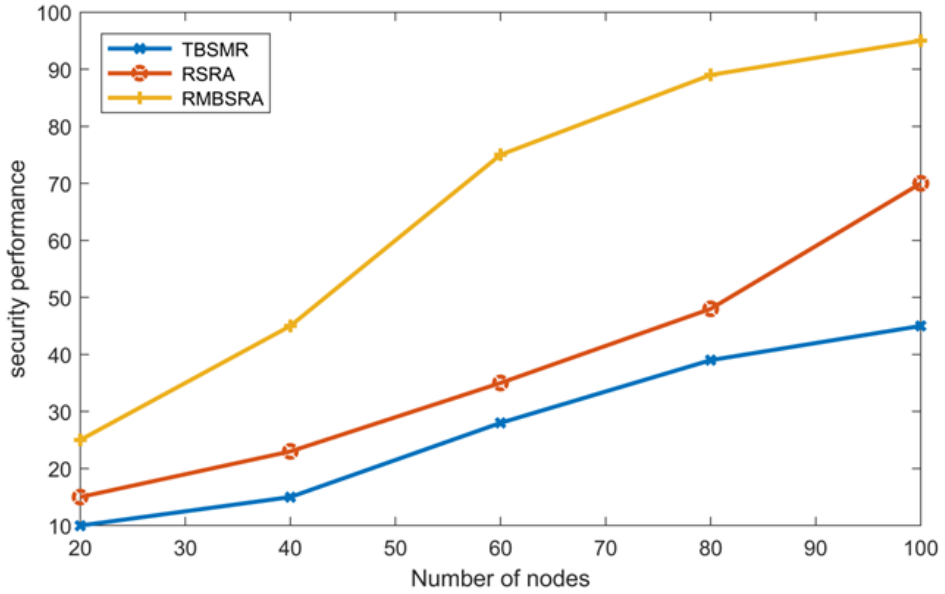

Figure 7 Security Performance Vs. Number of Nodes

Figure 5 describes the performance comparison between the proposed RMBSRA with TBSMR and RSRA. The evaluation metric discussed here is PDR, and it is calculated through a number of nodes involved with its achieved PDR in percentage. The X-axis shows the total nodes taking part in the experiment in which the node count is increased by 1 at regular intervals. The Y-axis shows the total PDR achieved by respective nodes. The proposed RMBSRA achieves a PDR of 26% for 1 node, 44% of PDR for 2 nodes, 75% of PDR for 3 nodes, 92% of PDR for 4 nodes, and 96% of PDR for 5 nodes. Whereas RSRA achieves a PDR of 14% for 1 node, 20% of PDR for 2 nodes, 34% of PDR for 3 nodes, 58% of PDR for 4 nodes and 70% of PDR for 5 nodes. The TBSMR achieves PDR of 10% for 1 node, 17% of PDR for 2 nodes, 28% of PDR for 3 nodes, 36% of PDR for 4 nodes and 45% of PDR for 5 nodes. It clearly shows the PDR achieved by the proposed RMBSRA is more efficient than the others.

The figure 6 describes the performance comparison between the proposed RMBSRA with TBSMR and RSRA. The evaluation metric discussed here is routing overhead, and it is calculated through a number of nodes involved with its routing overhead in hop count. The X-axis shows the total nodes taking part in the experiment in which the node count is increased by 20 at regular intervals. The Y-axis shows the total routing overhead achieved by respective nodes. The proposed RMBSRA has a 30 hop count for 20 nodes, 32 of hop count 40 nodes, 36 of hop count for 60 nodes, 60 of hop count for 80 nodes, and 120 of hop count for 100 nodes. Whereas the RSRA achieves has 48 hop count for 20 nodes, 52 of hop count 40 nodes, 140 of hop count for 60 nodes, 160 of hop count for 80 nodes, and 270 of hop count for 100 nodes. The performance achieved by TBSMR has a 60 hop count for 20 nodes, 120 of hop count 40 nodes, 170 of hop count for 60 nodes, 230 of hop count for 80 nodes, and 300 of hop count for 100 nodes. The above results on all the node range proposed RMBSRA has a minimum cop count than the others.

The figure 7 describes the security performance comparison between the proposed RMBSRA with TBSMR and RSRA. The evaluation metric discussed here is security performance, and it is calculated through the number of nodes involved with its security performance in percentage. The X-axis shows the total nodes taking part in the experiment in which the node count is raised by 20 at regular intervals. The Y-axis determines the total security performance achieved by respective nodes. The proposed RMBSRA has 25% of security performance for 20 nodes, 42% of security performance for 40 nodes, 70% of security performance for 60 nodes, 87% of security performance for 80 nodes, and 94 % of security performance for 100 nodes. Whereas RSRA achieves the security performance of 15 % for 20 nodes, 20 % for 40 nodes, 25% for 60 nodes, 34% for 80 nodes, and 65% for 100 nodes. Then the TBSMR achieves 10% for 20 nodes, 15 % for 40 nodes, 25% for 60 nodes, 26% for 80 nodes and 35% for 100 nodes. The observation graph clearly shows the security performance attained by RMBSRA is more efficient than the others.

5. CONCLUSION

The paper proposed routing manager-based secure rate analysis (RMBSRA) for MANET. The main motto of the proposed system is to achieve multipath routing system and

RESEARCH ARTICLE

overall optimum performance—the change of network which make network stability and security more challenging and task. To overcome this proposed system, we introduced Routing Manager (RM) as an essential component responsible for the overall network activities. RM collects all network activities and updates the information in the neighboring table. Based on the collected information, it organizes the multipath from source to destination. If any link failure occurs in the current path, an automatic alternative path is selected, and this process is continued until the packet reaches the destination. The neighboring table contains all node activity details and regularly updates the inactive and cooperative node lists. The communication using the active nodes performs effective results in comparison to the existing systems. A comparison work is carried out for determining the efficiency of the proposed RMBSRA with TBSMR and RSRA. The factors in determining the effective performance are PDR, throughputs, routing overhead, and security. The proposed RMBSRA results are far better than others in all the performance factors. Thus, it proves it is a more efficient multipath routing system than the existing systems.

5.1. Future Scope

In this paper, an effective and secure transmission is implemented using the proposed routing. However, to manage the increasing demand and higher security, future work should focus on enhancing data transmission security using authentication techniques.

REFERENCES

[1] B. Salah Eddine, S. Omar, B. Meftah, M. Rabbah, and B. Cousin, "An efficient energy-aware link stable multipath routing protocol for mobile ad hoc networks in urban areas," Telford Journal, vol. 12, pp. 2–7, 01 2020.

[2] S. K. Singh and J. Prakash, "Energy efficiency and load balancing in manet: A survey," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 832–837.

[3] A. Parveen and Y. V. S. Sai Pragathi, "A study of routing protocols for energy conservation in manets," in Advances in Decision sciences, Image Processing, Security and Computer Vision, S. C. Satapathy, K. S. Raju, K. Shyamala, D. R. Krishna, and M. N. Favorskaya, Eds. Cham: Springer International Publishing, 2020, pp. 641–647.

[4] Z. Chen, W. Zhou, S. Wu, and L. Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed manet," IEEE Access, vol. 8, pp. 44 760–44 773, 2020.

[5] M. Anand and T. Sasikala, "Efficient energy optimization in mobile ad hoc network (manet) using better-quality aodv protocol," Cluster Computing, vol. 22, 09 2019.

[6] L. Atzori, A. Iera, and G. Morabito, ―The internet of things: A survey,‖ Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[7] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, ―Convergence of MANET and WSN in IoT urban scenarios,‖ IEEE Sens. J., vol. 13, no. 10,pp. 3558–3567, Oct. 2013.

[8] Mohit K. and Rashmi Mishra. An Overview of MANET: History, Challenges and Applications. International Journal of Engineering Research and Technology. (2012). vol. 3, no.1.

[9] Pravin Ghosekar. 2010. Mobile Ad Hoc Networking: Imperatives and Challenges. In proceedings of IJCA, Special issues on "Mobile Ad-hoc Networks" (MANET).

[10] N. Sah, N. R. Prakash, and D. Bagai "QoS Analysis in Mobile AdHoc Networks Using Bandwidth Utilization Technique", Dec 2014.

[11] Karlsson, Jonny, Laurence S. Dooley, and Goran P. Pulkkis. "Secure Routing for MANET Connected Internet of Things Systems." (2018).

[12] Alameri, I. A. "MANETS and internet of things: the development of a data routing algorithm." Engineering, Technology & Applied Science Research 8, no. 1 (2018): 2604-2608.

[13] Mohammed Shabaz Hussain and Khaleel Ur Rahman Khan, "Network-based Anomaly Intrusion Detection System in MANETS," Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC 2020, IEEE Xplore Part Number: CFP20J06-ART; ISBN: 978-1-7281-2813-9

[14] Hui Lin, Jia Hu, Xiaoding Wang, Mohammed F. Alhamid and Md. Jalil Piran "Towards Secure Data Fusion in Industrial IoT using Transfer Learning", IEEE Transactions on Industrial Informatics 2020, DOI 10.1109/TII.2020.3038780, IEEE

[15] SIVASHANKARI RAJADURAI, MAMOUN ALAZAB, NEERAJ KUMAR AND THIPPA REDDY GADEKALLU, "Latency Evaluation of SDFGs on Heterogeneous Processors Using Timed Automata", IEEE Acess July 2020, Digital Object Identifier 10.1109/ACCESS.2020.3013013

[16] Mohammad Sirajuddin, Ch. Rupa , Celestine Iwendi and Cresantus Bamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network",Hindawi Security and Communication Networks Volume 2021, Article ID 5521713, 9 pages https://doi.org/10.1155/2021/5521713

[17] P. Sathyaraj and D. Rukmani Devi, "Designing the routing protocol with secured IoT devices and QoS over Manet using trust‑based performance evaluation method", Springer-Verlag GmbH Germany, part of Springer Nature 2020, Journal of Ambient Intelligence and Humanized Computing https://doi.org/10.1007/s12652-020-02358-4

[18] Swetha MS (2019) A novel approach to secure mysterious location based routing for Manet. IJITEE 8(7):2587–2591

[19] Belgaum MM (2019) Secured approach towards reactive routing protocols using triple factor in mobile ad hoc networks. AETiC 3(2):32–40

[20] Guaya-Delgado L (2019) A novel dynamic reputation-based source routing protocol for mobile ad hoc networks, vol 77. Springer, New York

[21] Mukhedkar MM (2019) Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm. Comput J 62(10):1528–1545

[22] Veeraiah N, Krishna BT (2020) An approach for optimal-secure multipath routing and intrusion detection in MANET. Evolutionary intelligence. Springer, New York

[23] Singh, K., & Gupta, R. (2021). SO-AODV: A Secure and Optimized Ad-Hoc On-Demand Distance Vector Routing Protocol Over AODV With Quality Assurance Metrics for Disaster Response Applications. Journal of Information Technology Research (JITR), 14(3), 87-103. http://doi.org/10.4018/JITR.202107010

[24] H. Kathiriya, A. Pandya, V. Dubay, and A. Bavaria, "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.

[25] 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

[26] 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.

[27] 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.

RESEARCH ARTICLE

[28] 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.

[29] 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.

[30] 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.

[31] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, ")e 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

[32] 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, 32.6, e3997, 2021.

Author

Dr. P. T. Kasthuri Bai (Pattabiram Thulasingam Kasthuri Bai) has obtained her Bachelor's degree in Mathematics from University of Madras. She has obtained her Master's degree in Computer Applications from Bharathidasan University, Master of Philosophy in Computer Science from Alagappa University. She qualified herself by passing UGC-NET and SET exams held in June 2012 and Oct 2012 respectively. She has been awarded the degree of Doctor of Philosophy in Computer Science in the year 2019 from Bharathiar University, Coimbatore. She has 16 years of teaching experience and 6 years of corporate experience. At present She is The Head & Associate Professor, Department of Computer Science, Thiruthangal Nadar College, Chennai. Her specializations include DBMS, Data Communication & Networks, Network Security, Routing in Mobile Adhoc Networks, Preventing attacks in MANETs, Improving the QoS parameters in MANETs etc. She has published 6 papers of which 3 are Scopus Indexed and one Science Citation Indexed (Wireless personal communication).

How to cite this article:

P.T. Kasthuri Bai, "RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 150-159, 2022, DOI: 10.22247/ijcna/2022/212331.