https://doi.org/ 10.33472/AFJBS.6.10.2024.3829-3839

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

An QoS Enabled Secure Routing Algorithm for Improved QoS in Manet

Dr.Shailesh Madhavrao Deshmukh,Assistant Professor, Department of Electrical, Kalinga University, Naya Raipur, Chhattisgarh, India.
ku.shaileshmadhavraodeshmukh@kalingauniversity.ac.in

Ravi Prakash Mahobia, Assistant Professor, Department of Electrical, Kalinga University, Naya Raipur, Chhattisgarh, India. ku.raviprakashmahobia@kalingauniversity.ac.in

Article History

Volume 6,Issue 10, 2024

Received:13 Apr 2024

Accepted : 05 May 2024

doi: 10.33472/AFJBS.6.10.2024.3829-3839

Abstract:

The quality of service of Mobile Adhoc Network (Manet) is greatly depending on the routing protocol enforced. There exists number of approaches to maximize the QoS of Manet. Some of the methods use the energy of nodes, mobility and other features, but still they compromise with various threats. Towards the problem, an QoS Enabled Secure Routing (QESR) is presented in this article. The method considers mobility speed, energy, directional density, transmission count, range and other features towards route selection. The method discovers routes by applying broadcast mechanism and collects above mentioned features. Further, the method computes different support measures like Reach Support, Throughput Support, Energy Scale Support values. Using these support values, QoS_Factor and Security Factor values are measured. Further, a secure transmission route is identified with the values measured. The method hikes secure routing and QoS performance.

Index Terms:

Manet, QoS, Secure Routing, QESR, QoS_Factor, Security Factor

1. Introduction:

Manet is the keen network being used in the world. The human society uses mobile phones for several communications and supports the access of different services to be performed through mobile devices. They access the internet through the devices and access other network services through the same. Manet performs data transmission with cooperative

transmission because of the restriction it has in terms of transmission range. The mobile node cannot transmit data packets directly to a service point or to a device which is located faraway from its communication range. To perform any data transmission, it identifies a route and forwards the data packet through number of intermediate mobile nodes, base station. Such cooperative transmission opens the gate for the network threat performed by number of malicious nodes.

To support the data transmission in Manet, there are number of routing protocols named in literature. The popular one is AODV (Adhoc On demand Distance Vector) routing, which discover the route between two mobile nodes and perform data transmission through intermediate nodes. Similarly, AOMDV, DSR,LEACH and other routing protocols are mostly used in Manet for better transmission. As the data packets are transmitted through intermediate nodes in the route, the malicious node present in the route perform eavesdrop, modification and other attacks. Presence of such attack degrades the service performance as well as the performance of entire network.

To handle the threats in the network, there are number of secure routing protocols are defined in literature. Some of the methods measure the trust of intermediate nodes according to their transmission history . There are few techniques, which indirectly gauge the trust of nodes like measuring the trust based on the residual energy and transmission involved. Similarly, the node trust is computed with retransmission, latency and throughput as well. However, the methods consider only limited parameters in measuring trust measurement. This increases the need of designing efficient secure routing protocol to support the QoS maximization of Manet.

The QoS of Manet is rely on the routing performance. If there is higher latency then it affects the throughput performance. Similarly, if there exist eavesdrop then it affects the throughput performance. If the malicious node chooses a longer route then it increases the throughput and affects the entire performance. Similarly, there are number of direct and indirect factors can be named which challenges QoS improvement. By considering all these issues, an efficient QoS Enabled Secure Routing (QESR) algorithm is sketched in this paper. The article dedicates the section 1 for the description of general introduction and section 2 details the literature around the problem. Section 3 briefs the working of proposed secure routing algorithm and section 4 comes with the results. Finally, section 5 briefs the summary of the work in detail.

2. Related Works:

There exists number of approaches towards secure routing in Manet. Set of methods among them are discussed in this part.

A Genetic algorithm with Hill climbing (GAHC) routing protocol is described in [1], which identifies the optimal route by clustering the nodes using fuzzy C-means algorithm according to the density of nodes. The route selection is performed by measuring the trust in direct and indirect way.

Bacteria for Aging Optimization Algorithm (BFOA) are presented in [2], which performs routing accoding to the trust and energy factors. Initially, fuzzy clustering scheme is applied to group the nodes and the trust of nodes is measured according to the trusts levels measured based

on latency, throughput, and connection within the course's boundaries. An authentication key management based secure cross layer routing scheme is presented in [3], which works according to the particle swarm optimization scheme. The method consider traffic index, energy, data rate and trust values. A secure intrusion detection system (S-IDS) is presented in [4], which performs secure routing to enforce secure intrusion detection in Manet. The method uses Secure Energy Routing (SER) scheme to perform efficient routing.

An Enhanced Energy Efficient-Secure Routing (EEE-SR) scheme is presented in [5], to support secure data access in hostile environment where the method uses security policy to enable data communication between nodes. A secure multipath routing scheme is presented in [6], which handles the distribution of loads by identifying maximum number of routes between two nodes to support routing on a low bandwidth conditions. Different methods of trust based routing for manet is reviewed in [7], which consider delivery ratio, energy efficiency and delay factors in route selection.

A trust orient scheme is briefed in [8], which uses atom whale optimization algorithm (AWOA), and consider average encounter rate (AER), and successful cooperation frequency (SCF), integrity factor towards measuring the trust of nodes. The trust based secure routing (TSR) model [9], uses hierarchical structure in identifying secure route towards data transmission. An secure dynamic on demand routing protocol (SDORP) is presented in [10], which identifies the secure route on the fly according to the energy and delivery ratio. An MSA-SFO-based Secure and Optimal Energy Routing Protocol is presented in [11], which uses neighbor trust data towards route selection.

A Position Update Secure Routing (PUSR) is presented in [12], which works according to AODV routing protocol with Prevention of Selfish Node using Hash Function (PSNHF) with position update algorithm in identifying the secure route.

RMBSRA: Routing Manager Based Secure Route Analysis is presented in [13], which uses bandwidth allocation and traffic as key in identifying the secure route. The issues present in Manet are presented in [14], which categorizes the issues and attacks in the network. A node authentication and trusted routing (NATR) model is presented in [15], towards identifying abnormal node interference. The method monitor the success rate of the nodes in measuring the trust to support secure routing. A path security and trust based AODV (ST_AODV) algorithm is presented in [16], which identifies the malicious node by analyzing the activity of the nodes to measure the trust level of nodes. Blockchain based secure routing scheme (Block_Sec) [17], uses Distributed One-Time Passcode (DOT) to perform authentication of nodes and uses Weight based Dynamic Clustering (WDC) algorithm to group the nodes to support secure routing. A secure routing protocol is presented in [18], which focused in reducing the routing overhead in secure Manet.

All the methods analyzed in the above section has the deficiency in achieving higher security performance and QoS achievement.

3. QoS Enabled Secure Routing (QESR) Model:

The proposed QoS Enabled Secure Routing (QESR) model receives the data packet and performs route discovery. Broadcasting method is used for discovering routes and other features. The method considers mobility speed, energy, directional density, transmission count, range and other features towards route selection. The method discovers routes by applying broadcast mechanism and collects above mentioned features. Further, the method computes different support measures like Reach Support, Throughput Support, Energy Scale Support values for each route identified. According to the different support values measured, the method estimates the value of QoS_Factor and Security Factor values. Using the values, the method computes the value of QSSupport value. Based on the value of QSSupport, an optimal secure route is selected and the packet has been transmitted through the route selected.

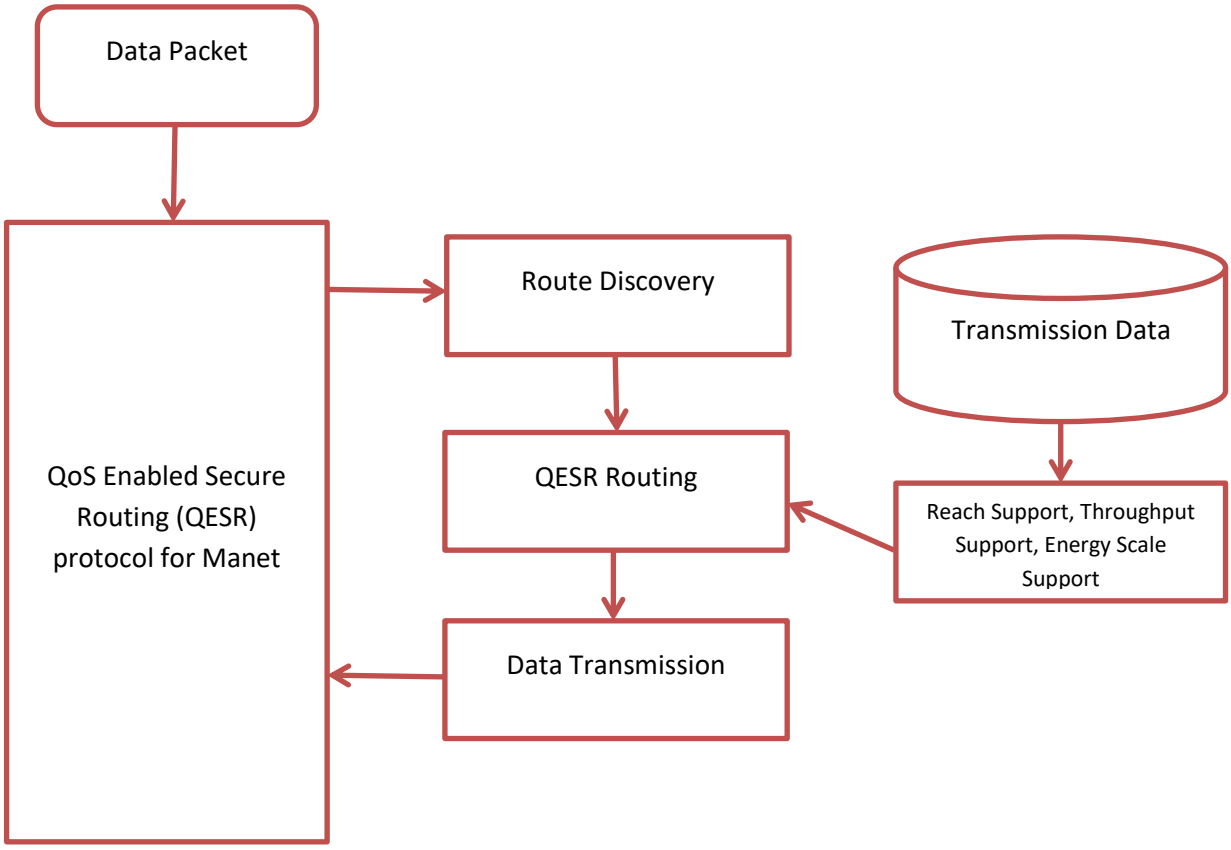

Figure 1: Block Diagram of Proposed QESR Routing Model

The working of proposed QESR routing model is given in Figure 1, and the functions are detailed in this section.

Route Discovery:

The proposed approach performs route discovery by generating route request QESR_RR packet. Generated route request packet is broadcasted in the network which has been flood throughout the network. Upon receiving the packet, the intermediate nodes verifies their route table for the presence of route. If there is an entry then it generates a route reply packet QESR_REP packet. With the route reply the nodes add their entry at the end and send back to

the source. With the same, the nodes add the features like residual energy, number of transmission performed, and number of neighbors. The source node receive the reply packet and extract the route as well as other features from the packet. Extracted features are updated to the route table and node table. The routes discovered are used to perform route selection towards data transmission.

Algorithm:

Given: Route Table RT, Node Table NT, Packet P, and Transmission Trace TT

Obtain: Route Table and Node Table, TT.

Start

Read RT, NT,P, TT.

$Size(RT)$

if $RT(i) \in P.Destination\ then$

$i = 1$

perform QESR Routing (RT, NT and TT)

else

Generate QESR_RR = {Source Id, P.Dest}

Broadcast QESR_RR packet.

While true

Receive QESR_RR packet.

$Size(RT)$

If $RT(i) \in QESR\_RR.Destination\ then$

$i = 1$

Generate QESR_RP packet.

QESR_RP={RT(i).Route+NodeId,NoT, RE,Nn,Ms}

Send QESR_RP towards source node.

Else

Add node id to the sequence.

Add NodeId,NoT,RE,NN,Ms to the sequence.

Broadcast the packet.

End

Receive QESR_RP packet.

Extract route and add to the route table.

For each hop in route

Extract NN,NOT, RE, Ms

//NN-number of neighbors, NoT – Number of transmission performed,RE – Residual Energy, Ms-mobility speed.

Add to the node table.

End

End

Stop

The route discovery algorithm identifies routes in the network and collects different features about the nodes to support data transmission.

QESR Routing:

The QoS enabled secure routing algorithm reads the set of entries from the route and node table. For each route available, the Reach support (RS), Throughput Support (Ths), Energy Scale Support (ESS) is measured. The values of RS, Ths, and ESS are used to measure QoS_support and Security_Support. Further, the QSS_Support value is measured with the use of above measures. A route with higher QSS_support is selected for data transmission.

Algorithm:

Given: Route Table RT, Node Table NT, Transmission Trace TT, Packet P.

Obtain: Null

Start

Read RT, NT,TT, P.

{RT,NT,TT} = Perform Route discovery (RT, NT, TT)

For each route r

Compute Reach Support RS.

$$Rs = \left(\frac{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).Nn?NT(i).id==r(i).Nodeid)}{size(r)} \times \frac{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).Ms?NT(i).id==r(i).Nodeid)}{size(r)}\right)$$

Compute Throughput Support Ts.

$$Ts = \frac{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).NoRT?NT(i).id==r(i).Nodeid)}{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).NoT?NT(i).id==r(i).Nodeid)}$$

Compute Energy Scale Support ESS.

$$ESS = \frac{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).RE\ ?\ NT(i).id==r(i).Nodeid)}{size(R)} \times \frac{\sum_{j=1}^{size(NT)} Count(\sum_{i=1}^{size(r)} NT(j).NoT?NT(i).id==r(i).Nodeid)}{size(r)}$$

Compute QoS_Support = $\frac{Ts}{RS} \times Ess$

Compute Security_Support = RS×Ess

Compute QSS_Support = QoS_Support×$\frac{Security\_support}{Size(r)}$

End

$$size(RT)$$

Route R = $Max(RT(i).QSS\_Support)$. Route

$$i = 1$$

Perform data transmission with the route selected.

Stop.

The working of QESR routing model is presented in the above pseudo code. The method finds set of routes and measure QSS_support value is measured according to various support values. A most effective route is selected for data transmission based on QSS_Support value.

4. Results and Discussion:

The proposed QoS Enabled secure routing algorithm QESR has been simulated with network simulator with varying nodes in the network. At each test case, the performance of the method is measured in various parameters and recorded.

Key	Value
Tool	Network Simulator 2
Number of Nodes	200
Simulation Time	20 seconds
Residual Energy	100 joules
Mobility Speed	0.5 meters / second

Table 1: Evaluation Details

The details of evaluation have been presented in Table 1, which has been used to measure the performance of the proposed model.

Secure Routing Performance %			
	50 Nodes	100 Nodes	200 Nodes
PSO	69	74	78
GAHC	72	77	83
TSR	75	79	87
QESR	82	91	98

Table 2: Secure Routing Performance

The efficiency of methods in secure routing produced by different methods are measured and given in in Table 2. The QESR routing algorithm achieves higher routing performance than others.

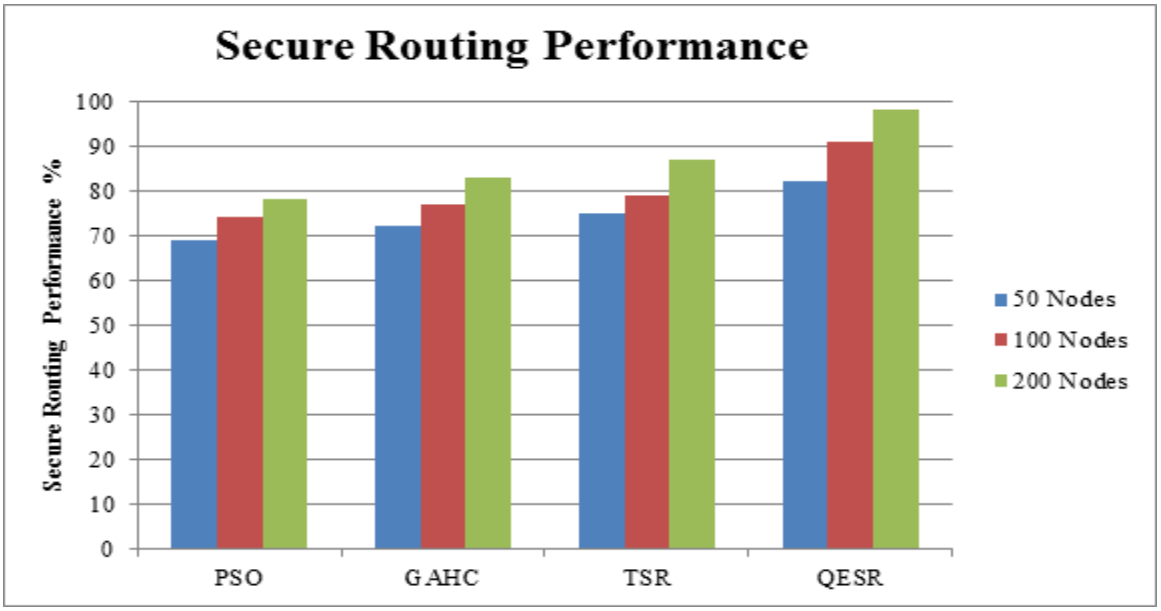

Figure 2: Secure Routing vs No of Nodes

The performance of the methods in secure routing is evaluated and given in Figure 2. The QESR model introduces higher performance compare to others.

Throughput Performance vs No of Nodes			
	50 Nodes	100 Nodes	200 Nodes
PSO	66	71	75
GAHC	69	74	78
TSR	73	78	83
QESR	81	89	95

Table 3: Analysis on Throughput Performance

The throughput achieved by various methods is given in Table 3, and QESR routing shows higher performance than others.

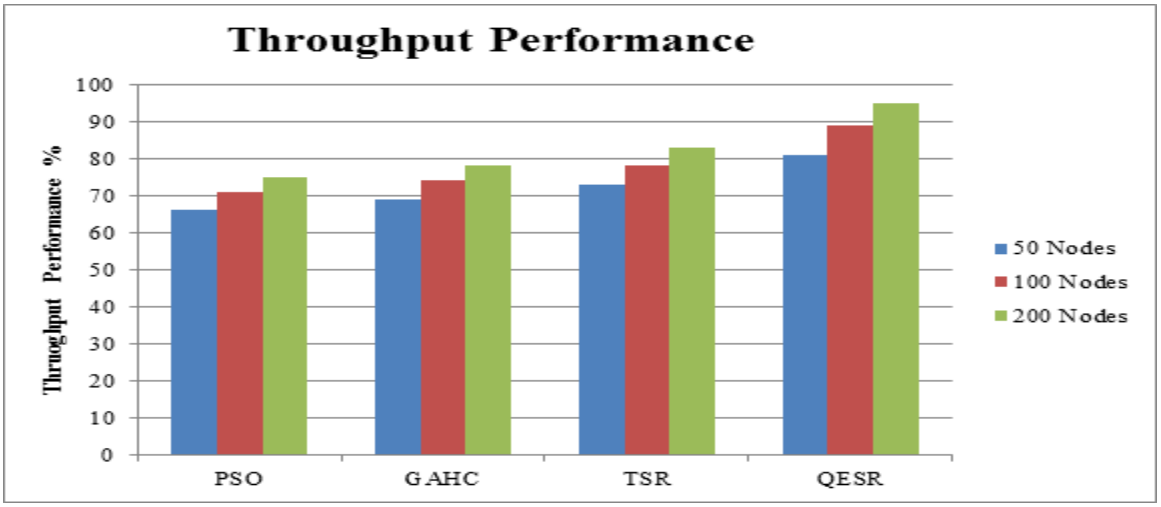

Figure 3: Throughput Performance

The throughput achieved by various routing algorithm are measured and plotted in Figure 3, and QESR shows higher achievement.

Latency in Millie Seconds vs No of Nodes			
	50 Nodes	100 Nodes	200 Nodes
PSO	89	81	75
GAHC	82	75	71
TSR	76	69	63
QESR	41	29	15

Table 4: Analysis on Latency

The latency in data transmission is measured and given in Table 4, and QESR routing shows less latency compare to others.

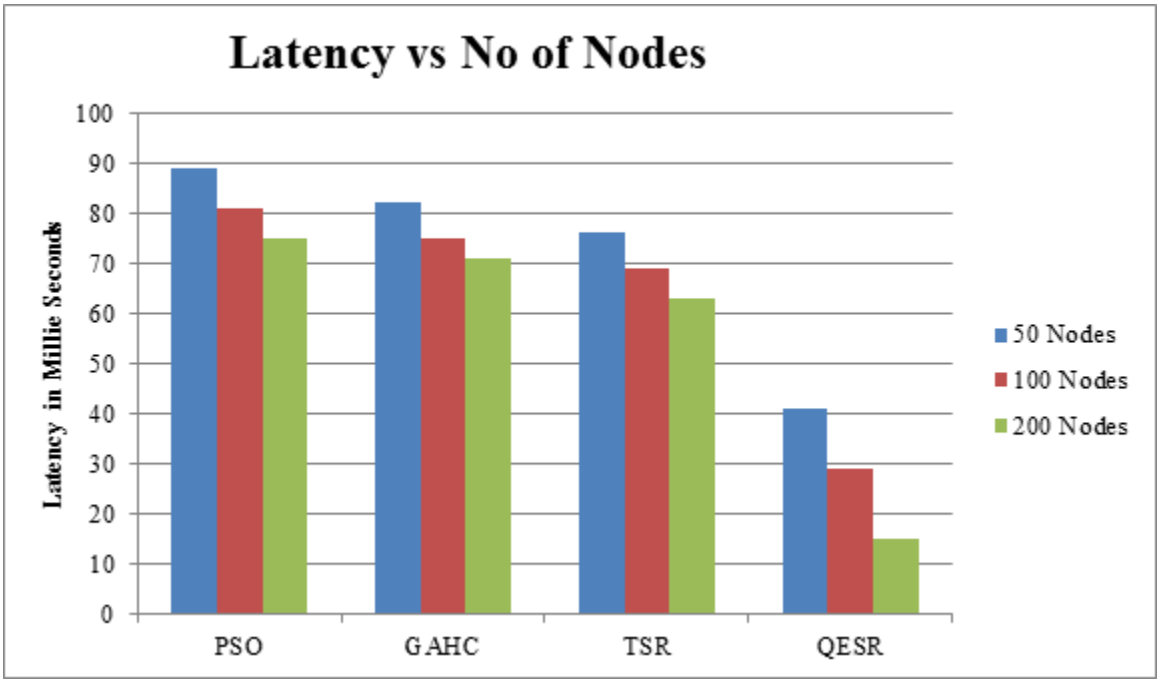

Figure 4: Latency vs No of Nodes

The value of latency introduced by the methods in data transmission is evaluated and QESR routing scheme shows less latency than others as per Figure 4.

5. Conclusion:

This paper presented a QoS Enabled Secure Routing (QESR) protocol for the support of Manet. The method performs route discovery initially and computes reach support, throughput support and energy scale support values. Based on these values, the method estimates QoS_Support and Security_support values. These values are used to measure the value of QSS_support based on which an optimal route is selected. The proposed method introduces higher performance in secure routing and QoS achievement.

References:

1. U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf and B. V. Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET," in *IEEE Access*, Volume. 9, pp. 163043-163053, 2021.
2. U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," in *IEEE Access*, Volume. 10, pp. 14260-14269, 2022.
3. G. R. Rama Devi, "Secure cross-layer routing protocol with authentication key management scheme for manets", ELSEVIER (M:S), Volume 29, Number 100869, 2023.
4. Rajendra Prasad P, "Secure intrusion detection system routing protocol for mobile ad-hoc network", Science Direct (GTP), Volume 3, Issue 2, PP 399-411, 2022.
5. Rajendra Prasad P, "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network", Science Direct (GTP), Volume 3, Issue 2, PP 412-423, 2022.
6. Tao Hai, Jincheng Zhou, "Enhanced security using multiple paths routine scheme in cloud-MANETs", Springer Open (JCC), Volume 12, Number 68, 2023.
7. Shalini Sharma, "A survey of trust based secure routing protocol used in mobile ad hoc networks", edp Sciences (ITM), Volume 54, Number 02009, 2023.
8. Suresh R. Halhalli; Shounak Rushikesh Sugave; B.N. Jagdale, "Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm", INDER SCIENCE (IJCN&DS), Volume 27, Number 1, 2021.
9. Anugraha, Krishnaveni, "An Efficient and Secure Routing in MANET using Trust Model", IJETT, Volume 70, Issue 9, 2022, PP 330-336.
10. K. Thamizhmaran, "Design Secure Routing Protocol for MANET", JR&AEE, Volume 3, Number 2, 2020.
11. D. Naga Tej, K.V. Ramana, "MSA-SFO-based Secure and Optimal Energy Routing Protocol for MANET", SAI (IJACSA), Volume 13, Issue 6, 2022.
12. Mallikarjuna Anantapur," PUSR: Position Update Secure Routing protocol for MANET", INASS (IJIE&S), Volume 14, Number 1, 2021.
13. P. T. Kasthuri Bhai, "RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET", IJCNA, Volume 9, Issue 2, 2022.
14. Ms V. Divya," Routing Protocol And Security Threats In Manet", IJS&TR, Volume 9, Issue 4, 2020.
15. M. Venkat Das, "Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET)", TJC&ME , Volume 12, Number 14, 2021, PP 5199-5211.
16. Vijaya Bhaskar .Ch, "AODV (ST_AODV) on MANETs with Path Security and Trust-based Routing", IJRITCC(A), Volume 10, Number 11, 2022.
17. N. Ilakkiya, "Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks", IJCC&C(A), Volume 18, Number 2, 2023.

18. R. Pravallika, G. Anushka, “Reducing the Routing Overhead in Secure Mobile AD HOC Networks”, IJERT, Volume 9, Issue 5, 2020.