Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.032239
Article

Tech Science Press

Region Centric GL Feature Approximation Based Secure Routing for Improved QoS in MANET

S. Soundararajan[1], R. Prabha[2], M. Baskar[3,*] and T. J. Nagalakshmi[4]

[1]Velammal Institute of Technology, Tamilnadu, 601 204, India
[2]Sri Sairam Institute of Technology, Tamilnadu, 600 044, India
[3]SRM Institute of Science and Technology, Chengapattu, Tamilnadu, 603 203, India
[4]Saveetha School of Engineering, Tamilnadu, 600 124, India
*Corresponding Author: M. Baskar. Email: baashkarcse@gmail.com
Received: 11 May 2022; Accepted: 21 June 2022

Abstract: Secure routing in Mobile Adhoc Network (Manet) is the key issue now a day in providing secure access to different network services. As mobile devices are used in accessing different services, performing secure routing becomes a challenging task. Towards this, different approaches exist which find the trusted route based on their previous transmission details and behavior of different nodes. Also, the methods focused on trust measurement based on tiny information obtained from local nodes or with global information which are incomplete. However, the adversary nodes are more capable and participate in each transmission not just to steal the data also to generate numerous threats in degrading QoS (Quality of Service) parameters like throughput, packet delivery ratio, and latency of the network. This encourages us in designing efficient routing scheme to maximize QoS performance. To solve this issue, a two stage trust verification scheme and secure routing algorithm named GL-Trust (Global-Local-Trust) is presented. The method involves in route discovery as like popular AODV (Adaptive On-demand Distance Vector) which upgrades the protocol to collect other information like transmission supported, successful transmissions, energy, mobility, the number of neighbors, and the number of alternate route to the same destination and so on. Further, the method would perform global trust approximation to measure the value of global trust and perform local trust approximation to measure local trust. Using both the measures, the method would select a optimal route to perform routing. The protocol is designed to perform localized route selection when there is a link failure which supports the achievement of higher QoS performance. By incorporating different features in measuring trust value towards secure routing, the proposed GL-Trust scheme improves the performance of secure routing as well as other QoS factors.

Keywords: MANET; secure routing; two stage trust; GL-trust; quality of service

1 Introduction

The recent development in information and communication technology has encouraged the human society to access different services and applications through mobile devices. The service providers provide number of services for the mobile users through which they can access vast services to perform various tasks. Such service data has been transferred to the service point and the result has been returned to the mobile user. But, the mobile nodes cannot communicate directly with the service point which makes them to perform cooperative transmission. Mobile Adhoc Network (MANET) has been framed with number of mobile devices, a set of static nodes as base stations. The mobile nodes have set of properties like mobility-in which the node has no restriction, energy- limited energy given to the mobile node. The mobility nature of the mobile nodes introduces topology changes which introduces several challenges. However, to access the service point, the mobile nodes involve in cooperative transmission to handover the data packets. Such deficiency in data transmission enables the way for the adversaries to involve in different threats.

The nature of data transmission opens the gate for the malicious node to perform several network threats. For example, when there is a malicious node present in a transmission route, it would involve in different threats like Eavesdrop (simply dropping packets), Selective forwarding (drops selective packets), DDoS (Distributed Denial of Service) attack, Sink hole attack and black hole attack. Whatever the threat, it directly affects the quality of service of the entire network. So, the quality of service of the MANET is greatly depending on how the routing is performed. Secure routing is the process of finding secure route and forwarding the data packets through the route selected.

As the MANET t is subject to topology changes, there will be link failure which increases the latency and reduces the throughput performance. There are number of secure routing schemes available, for example, Energy based routing schemes are used to identify secure route based on the energy of routes and number of transmission performed. But the adversary is capable of containing higher energy and participates on almost all the transmission and performs the attack. Similarly, location based approaches are used in verifying the trust of nodes but the adversary nodes would specify fake location details to overcome this. Behavior based approaches are used in different methods but the efficiency is depend on the availability of transmission traces. The latency based approach are available which measure the average latency and based on that a secure route would be identified. However, all the methods suffer with poor performance in secure routing. But in reality, QoS (Quality of service) of any network is greatly depending on various parameters which are interlinked. By achieving higher throughput performance the QoS of the network would be improved which depend on reduced latency; higher secure routing, and so on. So, by increasing the secure routing performance and by choosing least latency route, the throughput performance can be improved and also packet delivery ratio will be hiked. Among other factors, secure routing has higher importance because if the threats are not handled properly, there will be higher packet drop, the malicious nodes would divert the nodes through longer route to increase the latency which in turn would reduce the packet delivery ratio and throughput and affects the QoS performance. Secure routing is performed with several ways by identifying least hop count, least latency route, and by identifying behavior of nodes, by finding higher throughput route. Also secure routing is performed by measuring trust of routes based on various parameters of routes and the hops present.

On the other side, the trust based approaches can be used in secure routing. But the verification of trust must be performed in different ways. This article discusses such approach named GL-Trust (Global Local Trust) which measures trust in two ways. Global trust is the measure which represents the trust of any route and nodes on the route. The global trust can be computed based on the parameters like energy, mobility, number of transmissions. When a route has set of nodes with proportional energy according to the number of transmission with least mobility, then it can be considered for data transmission. On the other side, the local trust is the measure which represents the trust of node within the region or least

number neighbor hops. If a specific node is considered for number of transmission by neighbors repeatedly, then it can be considered that the specific node would be more legitimate in transmission and considered by neighbors. According to these two corollaries, the proposed methods would measure the global trust and local trust for different routes to perform secure routing. By measuring the trust of route in two stages as global and local, the security performance can be improved and would maximize the QoS performance. The detailed approach has been discussed in the next sections.

2 Related Works

There exist several routing schemes around the problem of secure routing in MANET. This section details set of approaches related to the problem considered.

A QoS constraint routing is presented in [1], which finds the valid route at route failure in such a way to maximize QoS performance. A proactive NOLSR (New Optimized link state routing) approach is presented for NDN (Named Data Network) network in [2], which perform routing according to the link state. A 3 dimensional logical identifier space (3D-LIS) is presented in [3], which uses structure of different nodes in efficient routing. A location aware routing towards delay tolerant network (LAROD) is presented in [4], which uses beaconless strategy and location towards efficient routing. A topology adaptive Ad-hoc on demand routing (TA-AOMDV) is presented in [5], towards maximizing QoS even at higher mobility speed of nodes. The method uses node resources as well as link stability in route selection. An active authentication scheme (AAS) is discussed in [6], which works based on the characteristics of active routing protocols towards various attacks. An evolutionary self-cooperative trust (ESCT) scheme is presented in [7], where the nodes shares trust information between them to perform effective routing.

A back propagation AODV (BP-AODV) is presented in [8], towards mitigating cooperative black hole attack. A machine learning based routing protocol towards maximizing QoS is presented in [9], which selects optimal route according to the behavior of nodes and uses regression technique. A zone-based route discovery mechanism (ZRDM) is presented in [10], which incorporates a link failure prediction mechanism (LFPM). The method handles the link failure and performs efficient routing.

A Constructive Relay based Cooperative Routing (CRCPR) is presented in [11], which uses topological information and energy, link stability in route selection. A novel Fitness function (FF-AOMDV) is presented in [12], which uses energy factor as fitness function parameters to perform path selection. A Q-learning based Traffic aware routing (QTAR) is presented in [13], which performs geographic routing according to static road map data. A QoE (Quality of Experience) orient multipath TCP routing scheme is presented as (MPTCP) in [14], which consider the connection state in different cycle to perform route selection. A link disjoint multipath routing scheme is presented in [15], which uses real-time condition in route selection. A smooth mobility and link reliability based routing (SMLR-OLSR) is presented in [16] which perform route selection according to the behavior of nodes, link condition and mobility. An energy efficient stable routing scheme with learning automata theory is presented in [17], which uses feedback factor to perform route selection. A novel Decasteljau algorithm is presented in [18], towards multipath routing in MANET, which uses mobility speed as the key in identifying the optimal route. An invariant packet feature based low rate attack detection scheme is presented in which uses network conditions in finding the optimal route to mitigate low rate distributed denial of service attacks. In an efficient integrated secure system is presented to include IoT (Internet of Things) devices and discusses efficient secure routing scheme. In a multi threshold traffic monitoring scheme to detect low rate DDoS attack is presented. The method uses traffic conditions in efficient route selection. In an efficient healthcare monitoring scheme is presented which uses efficient routing scheme to include IoT devices to support the monitoring process. A multi-feature learning model is presented in [19], which performs identification of vehicles with local attention to support secure data handover. A light weight convolutional neural network based fine grained vehicle

classification is presented in [20], which uses joint learning strategy and perform optimized feature selection towards classification.

All the methods discussed above suffer to achieve higher performance in routing in mobile adhoc routing to meet higher QoS performance.

3 Region Centric GL Feature Approximation Based Secure Routing

The proposed GL Trust approach performs routing based on the route discovery made by the approach initially. At initial stage, the method perform route discovery by overriding the popular AODV algorithm. More than AODV, the method collects different information from the hops of various routes. Discovered routes are further analyzed for their global trust by the source node according to different metrics of node and network conditions. Similarly, each route has been measured for the local trust by the intermediate nodes according to the trust of node among the neighbors. Using both the trust measures, the method would compute the value of Trusted Transmission Score (TTS). According to the value of TTS, a single route has been selected for data transmission. The complete method is discussed in this section.

The functional architecture of proposed GL-Trust Routing model is presented in Fig. 1, which has been detailed in component level in this section.

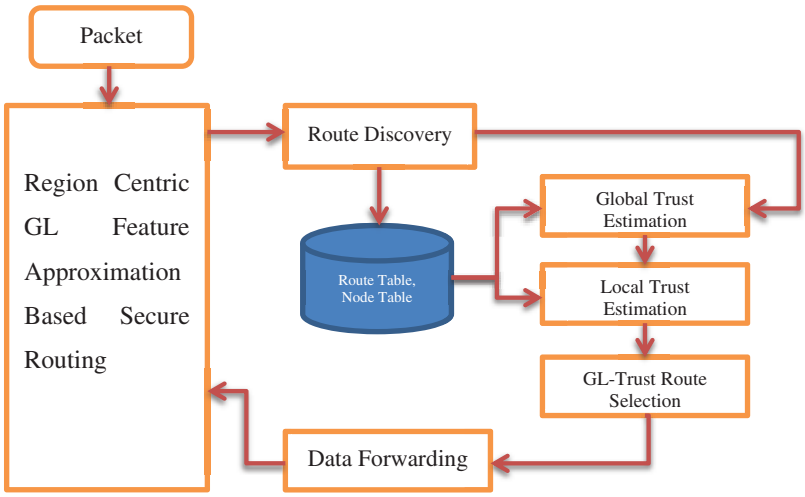

Figure 1: Architecture of GL-trust routing model

3.1 GL-Trust Route Discovery

The routes present and available between any source and destination are collected in this procedure. The method follows the same procedure of route discovery in AODV where it differs with the reply by fetching different other information than route in the reply packet. To perform this, the source node generates GL-RREQ message which is a route request message similar to RREQ (Route Request) message in AODV with source and destination addresses. Generated packet has been broadcasted in the network which has been received by the neighbors of the source and verifies their node and route table for the presence of route to reach the destination. If there is a route or the destination is located in the neighbor table, then it generates a GL-RREP message with positive tag. Also, the reply packet has been added with different other information like mobility speed, energy, number of transmission performed; number of neighbors and so on. Such tagged data with the packet has been sent to the source. The source receives all the

packets and fetches route and features of the hop to add to the table. Updated route and node table are used in further analysis to perform secure routing.

Algorithm:

Given: Node Table NT, Route Table RT, Packet P.

Obtain: NT, RT.

Start

Read NT, RT, P.

If P.Destination $\ni NT \&\& RT(i) \ni P.Destination$ $^{size(RT)}_{i=1}$ then

Generate GL-RREQ = {P.Source, P.Destination}

Broadcast GL-RREQ and Initialize Broadcast Timer.

While Timer Runs

Neighbors receives GL-RREQ.

If .Destination$\in NT \&\& RT(i) \in P.Destination$ $^{size(RT)}_{i=1}$ then

Generate GL-RREP={Source,Destination,MS,E,NoT,NoN,NoST,NoSpT}

Send GL-RREP to source.

Else

Forward the packets to its neighbors.

End

Source Receives route reply GL-RREP.

Extract Route R = $Route \in GLRREP$

RT = $\sum(Routes \in GLRREP) \cup R$

For each hop H

Extract mobility speed Ms.

Extract Energy E.

Extract Number of Transmission NoT.

Extract Number of Neighbors NoN.

Extract Number of self transmissionNoST.

Extract Number of supportive transmission NoSpt.

Add to node table NT.

End

End

Stop

The route discovery algorithm identifies a set of routes available between different nodes and fetches various features of the nodes of the route. Such route discovered and features extracted are updated to the route table and node table to support secure routing.

3.2 Global Trust Estimation

The global trust of any route represents the trustworthy of route according to global nature. Any route would have k number of hops and each have their own features like mobility speed, energy, transmission and so on. However, when they all clubbed as a route, the trust of the route should be measured for a secure routing. It can be measured based on various factors like energy, mobility, transmission and so on. To perform this, the method finds a set of hops present in a route R given and for each of the hop h, the method estimates Global Energy Trust (GET), Global Mobility Trust (GMT), and Global Transmission Trust (GTT). The value of GMT is measured based on the mobility speed of the node, when a node has a mobility value below average, then it can be considered as trusted node. Also, when a route has maximum nodes with least mobility rate than average then it can be considered that the entire route is trusted one. Similarly, GET is measured based on the average value of energy of all the nodes in the route. GTT is measured based on the number of successful transmission of nodes among number of transmission involved. Using all these trust values, the value of Global Trust (GT) is measured. Measured value of GT has been used to perform secure routing.

Algorithm:

Given: Route R, Node Table NT, Transmission Trace TT.

Obtain: GT.

Start

Read R, NT, RT.

Find list of hops Rhl = $\sum Hops \in R$

For each hop H

Compute Energy rate Er = Dist($\frac{InitialEnergy}{100}, \frac{NoT(H) \times \mu}{Initial\ Energy}$)

If Er>0 then

Er = 1

Else

Er = 0.

End

End

Compute Global Energy Trust GET = $\frac{\sum ER}{size(Rhl)}$

Compute average mobility Amr = $\frac{\sum_{i=1}^{size(Nhl)} Nhl(i).mobilityspeed}{size(Nhl)}$

Compute Global Mobility Trust GMT = $\frac{\sum_{i=1}^{size(Nhl)} Nhl(i).MobilitySpeed < Amr}{size(Nhl)}$

Compute Global Transmission Trust GTT = $\frac{\sum_{i=1}^{size(TT)} TT(i).State == Success \quad TT(i).Route == R}{\sum_{i=1}^{size(TT)} \quad TT(i).Route == R}$

Compute Global Trust GT = $\frac{GET}{GMT} \times GTT$

Stop

The method estimates the global trust by computing the trust of route on energy, mobility and transmission. According to the factors of various factors, the method computes the value of global trust to perform secure routing.

3.3 Local Trust Estimation

Local trust is the measure which represents the trust of a route upon nodes within the region or area considered. The trusts of nodes are measured according to the reputation of node among its neighbors. Even though there exist number of neighbors, how other nodes considered the node n for specific transmission. Also, the route must be flexible in choosing alternate route even there is a link failure. It can be approximated according to the number of neighbors a node has. Also, it is necessary to consider, how many number of transmission a node N performed, how many of them belongs to it own, and how many of them are belongs to others. The method computes the Neighbor Trust Factor (NTF) based on the number of nodes of the route present in the neighbor list of the source node and total nodes of the route. Also, the method computes the Transmission Associate Factor (TAF) based on the number of routes it has to reach the destination and total number of nodes present in the route. The value of Transmission Support Factor (TSF) is measured based on number of successful transmission made by the node and number of participation on other successful transmission. Finally Transmission Trust Factor (TTF) is measured based on the ratio of total successful transmission and total transmission involved. According to all these, the method computes the local trust (LT) to support secure routing. The value of Neighbor Trust Factor

Algorithm:

Given: Route R, Node Table NT, Transmission Trace TT.

Obtain: Local Trust LT.

Start

Read R, NT, TT.

Find hop list Hlist = $\sum Hops \in R$

For each hop H

Find Neighbor list Nlist = $\sum Neighbor(H) \in NT$

Compute Neighbor Trust Factor NTF = $\frac{\sum_{i=1}^{size(TT)} TT(i).Route \in Nlist.Any \;\; TT(i).Route \in H}{\sum_{i=1}^{size(TT)} TT(i).Route \in Nlist.Any}$

Compute Transmission Associate Factor TAF = $\frac{\sum Routes \rightarrow (H, Destination)}{H.NoN}$

Compute Transmission support factor TSF = $\frac{H.NoST}{H.NoT} \times \frac{H.NoSpT}{H.NoT}$

Compute Transmission Trust Factor TTF = $\frac{\sum_{i=1}^{size(TT)} TT(i).Route \in H \;\; TT(i).State == Success}{H.NoT}$

End

Compute LT = $\frac{\sum_{i=1}^{size(Hlist)} Hlist(i).NTF}{\sum_{i=1}^{size(Hlist)} Hlist(i).TAF} \times \frac{\sum_{i=1}^{size(Hlist)} Hlist(i).TTF}{\sum_{i=1}^{size(Hlist)} Hlist(i).TSF}$

Stop

The above discussed algorithm represents how local trust of the route is measured. It has been measured by computing neighbor trust factor NTF, transmission associate factor (TAF), Transmission support factor (TSF) and transmission trust factor (TTF). Using all these factors, the method computes the local trust to perform secure routing.

3.4 GL-Trust Route Selection

The global and local trust based route selection scheme discovers the routes between any source and destination. Further, the method would estimates global trust for each route identified and estimates local trust for the same. Using both the measures, the method computes Trusted Route Factor (TRF). Using the value of TRF, the method selects a single route to perform data transmission.

Algorithm:

Given: Packet P, Node Table NT, Route Table RT.

Obtain: Null.

Start

Read P, NT, RT.

Route list Rl = perform route discovery.

For each route R

GT = Estimate Global Trust.

LT = Estimate Local Trust

Compute Trusted Route Factor TRF = GT×LT

End

Route R = Choose most weighted route.

Perform data transmission.

Stop

The above discussed algorithm performs route discovery to find the routes. Accordingly, the method computes the global and local trust to select an optimal secure route to perform data transmission.

4 Results and Discussion

The proposed global local trust based secure routing scheme has been implemented using NS2. The performance of the method has been evaluated using various simulation scenario considered. Obtained results are compared with the results of other approaches. This section presents the analysis in detail.

The performance evaluation of proposed approach is performed according to the simulation constraints mentioned in Tab. 1. Accordingly, the results obtained are compared with the result of other approaches.

The efficiency of GL-Trust algorithm is measured with different nodes in the network and plotted in Tab. 2, where GL-Trust scheme has topped the routing performance up to 96%. This is much higher than the other schemes produces. Inclusion of proposed GL-Trust routing scheme support the achievement of higher routing performance as it select a route according to GL-Trust measures computed based on various factors.

Table 1: Evaluation details

Parameter	Value
Tool Used	NS2
Total Nodes	150
Energy	100 Joules
Simulation Area	1000 meters

Table 2: Analysis on routing performance

Routing performance			
	50 Nodes	100 Nodes	150 Nodes
CRCPR	65	69	75
QTAR	69	74	78
MPTCP	73	78	83
SLR_OLSR	81	85	88
GL-Trust	84	87	96

Efficiency of proposed GL-Trust approach is measured on routing and compared against the same with different approaches in Fig. 2. However, the GL-Trust scheme has produced noticeable growth on routing efficiency. The routing performance is improved because the selection of route is performed based on mobility trust, energy trust being computed on local and global level. This support the selection of secure route to perform data transmission. Also increasing number of nodes in the network support the availability of more number of routes which support the selection of most secure route to achieves higher QoS performance.

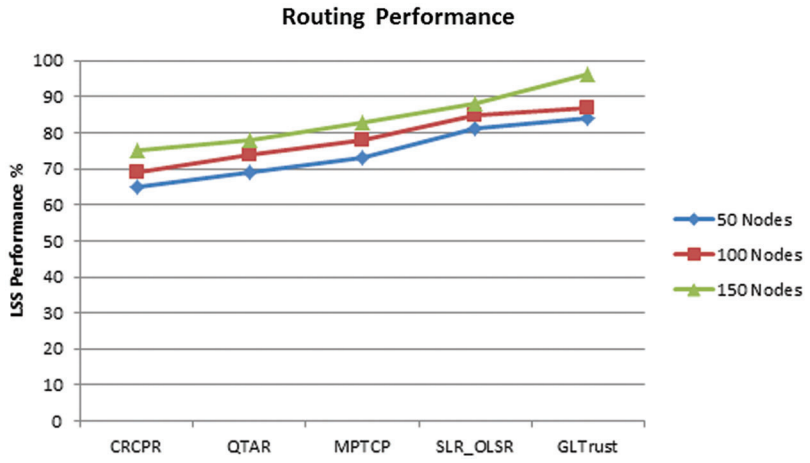

Figure 2: Analysis on routing performance

Efficiency of GL-Trust approach is measured against throughput achievement and achieves higher performance compare to rest of the techniques; it's shown in Tab. 3. By choosing a secure route with the proposed approach, the throughput performance is improved because, the method selects a most secure route according to transmission trust measures also. So, the method selects a most secure route to support effective transmission which supports the achievement of higher throughput.

Table 3: Analysis on throughput performance

	Throughput performance		
	50 Nodes	100 Nodes	150 Nodes
CRCPR	67	70	74
QTAR	69	74	78
MPTCP	71	77	82
SLR_OLSR	79	84	87
GL-Trust	82	88	97

Achieving throughput by different approaches are measured and plotted in Fig. 3, where GL-Trust scheme has introduced noticeable hike in the parameter than others. The increasing number of nodes in the network would provide number of nodes and possible to identify least mobility routes to support the achievement of higher throughput.

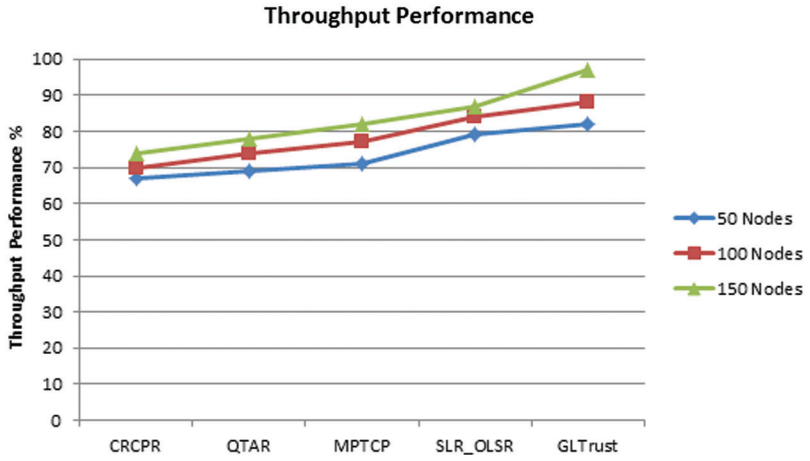

Figure 3: Analysis on throughput performance

The performance of the methods are measured on packet delivery ratio and compared with other methods, it's shown in Tab. 4. The proposed GL-Trust algorithm has produced higher packet delivery than other methods. By choosing most secure route with the proposed approach, the packet delivery ratio can be improved because it choose a most secure route according to various parameters.

Table 4: Analysis on packet delivery ratio

Packet delivery ratio %			
	50 Nodes	100 Nodes	200 Nodes
CRCPR	69	72	74
QTAR	71	74	76
MPTCP	74	78	81
SLR_OLSR	82	86	89
GL-Trust	85	89	98

The performance of packet delivery ratio produced by various approaches are measured and compared in Fig. 4. The proposed GL-Trust has produced higher packet delivery ratio than other approaches.

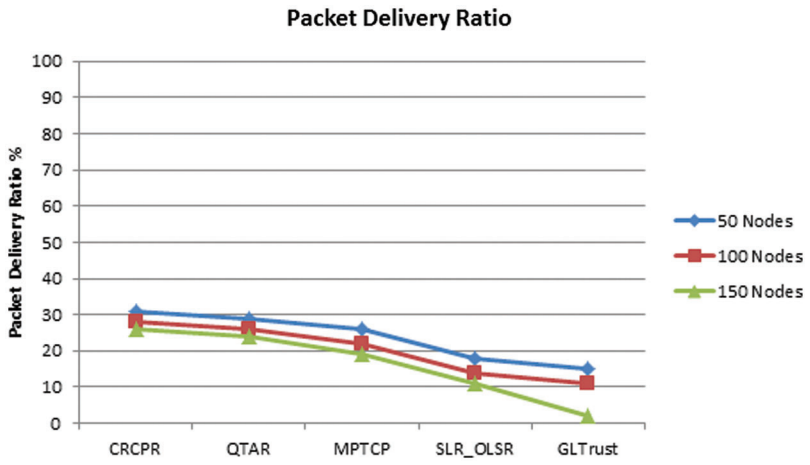

Figure 4: Analysis on packet delivery ratio

The ratio of packets being dropped by different approaches are measured and plotted in Tab. 5. The GL-Trust scheme has introduced negligible drop compare to others. The inclusion of proposed approach reduces the packet drop ratio because it handles number of threats successfully.

Table 5: Analysis on packet drop ratio

Packet drop ratio %			
	50 Nodes	100 Nodes	150 Nodes
CRCPR	31	28	26
QTAR	29	26	24
MPTCP	26	22	19
SLR_OLSR	18	14	11
GL-Trust	15	11	2

The ratio of packets being dropped by various approaches are measured and compared in Fig. 5, where GL-Trust scheme has produced less packet drop than others.

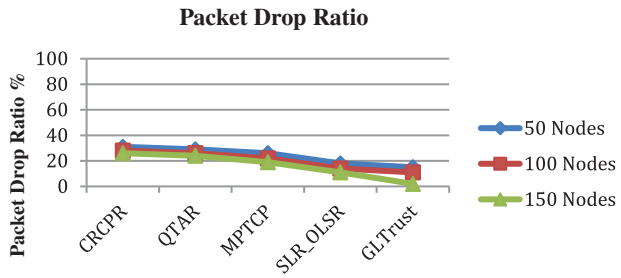

Figure 5: Analysis on packet drop ratio

The latency ratio introduced in packet transmission by various approaches are measured and presented in Tab. 6. The GL-Trust scheme has introduced negligible less latency compare to others.

Table 6: Analysis on latency in millie seconds

Latency in millie seconds			
	50 Nodes	100 Nodes	150 Nodes
CRCPR	67	64	59
QTAR	64	61	55
MPTCP	56	51	49
SLR_OLSR	43	35	29
GL-Trust	28	19	7

The latency ratio of transmitting packets is measured and compared in Fig. 6, where GL-Trust scheme has produced less latency than others.

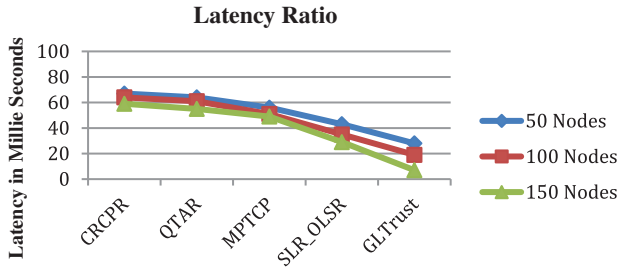

Figure 6: Analysis on latency ratio

5 Conclusion

In this paper, an efficient region centric GL approximation based secure routing is presented. The method discovers a set of routes between the source and destination. With the routes identified, the method estimates the global trust and local trust according to the multiple features. Based on the value of GL trust, the method estimates the trust factor. Based on the value of trust factor, the method chooses optimal route to perform data transmission. The method improves the performance of all the QoS

parameters than other approaches. The method achieves routing performance up to 96%, throughput performance up to 97%, packet delivery ratio up to 98% and packet drop ratio has been reduced up to 2% where the latency is reduced to 7 Millie seconds. The inclusion of proposed approach supports the higher achievement of QoS performance in overall.

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

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

References

[1] S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault-tolerant routing in MANETs," *China Communications*, vol. 12, no. 8, pp. 93–110, 2015.

[2] X. Guo, S. Yang, L. Cao, J. Wang and Y. Jiang, "A new solution based on optimal link-state routing for named data MANET," *China Communications*, vol. 18, no. 4, pp. 213–229, 2021.

[3] S. A. Abid, M. Othman and N. Shah, "Exploiting 3D structure for scalable routing in MANETs," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2056–2059, 2013.

[4] E. Kuiper and S. N. Tehrani, "Geographical routing with location service in intermittently connected MANETs," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 592–604, 2011.

[5] 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. 44760–44773, 2020.

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

[7] R. J. Cai, X. J. Li and P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42–55, 2019.

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

[9] D. Nayab, M. H. Zafar and A. Altalbe, "Prediction of scenarios for routing in MANETs based on expanding ring search and random early detection parameters using machine learning techniques," *IEEE Access*, vol. 9, pp. 47033–47047, 2021.

[10] B. H. Khudayer, M. Anbar, S. M. Hanshi and T. Wan, "Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks," *IEEE Access*, vol. 8, pp. 24019–24032, 2020.

[11] J. Bai, Y. Sun, C. Phillips and Y. Cao, "Toward constructive relay-based cooperative routing in MANETs," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1743–1754, 2018.

[12] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function," *IEEE Access*, vol. 5, pp. 10369–10381, 2017.

[13] J. Wu, M. Fang, H. Li and X. Li, "RSU-assisted traffic-aware routing based on reinforcement learning for urban vanets," *IEEE Access*, vol. 8, pp. 5733–5748, 2020.

[14] T. Zhang, S. Zhao and B. Cheng, "Multipath routing and MPTCP based data delivery over manets," *IEEE Access*, vol. 8, pp. 32652–32673, 2020.

[15] Y. H. Robinson, "Link-disjoint multipath routing for network traffic overload handling in mobile ad-hoc networks," *IEEE Access*, vol. 7, pp. 143312–143323, 2019.

[16] Z. Li and Y. Wu, "Smooth mobility and link reliability based optimized link state routing scheme for MANETs," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1529–1532, 2017.

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

[18] P. K. Pattnaik, B. K. Panda and M. Sain, "Design of novel mobility and obstacle-aware algorithm for optimal MANET routing," *IEEE Access*, vol. 9, pp. 110648–110657, 2021.

[19] W. Sun, X. Chen, X. R. Zhang, G. Z. Dai, P. S. Chang *et al.,* "A multi-feature learning model with enhanced local attention for vehicle re-identification," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3549–3560, 2021.

[20] W. Sun, G. C. Zhang, X. R. Zhang, X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30803–30816, 2021.