Received: 11 October 2023 | Revised: 12 January 2024 | Accepted: 20 January 2024
DOI: 10.1111/exsy.13561

ORIGINAL ARTICLE

Expert Systems WILEY

Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities

Ramesh Kait[1] | Sarbjit Kaur[2] | Purushottam Sharma[3] | Chhikara Ankita[1] | Tajinder Kumar[4] | Xiaochun Cheng[5]

[1]Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India
[2]Computer Science Department, Govt PG College, Ambala Cantt, India
[3]Department of Information Technology, ASET, Amity University Uttar Pradesh, Noida, India
[4]Computer Science Department, JMIETI, Radaur, India
[5]Computer Science Department, Swansea University, Swansea, UK

Correspondence
Purushottam Sharma, ASET, Amity University Uttar Pradesh, Noida, India.
Email: psharma5@amity.edu

Xiaochun Cheng, Computer Science Department, Swansea University, Swansea, UK.
Email: xiaochun.cheng@swansea.ac.uk

Abstract

Due to the characteristics of vehicular ad hoc networks, the increased mobility of nodes and the inconsistency of wireless communication connections pose significant challenges for routing. As a result, researchers find it to be a fascinating topic to study. Furthermore, since these networks are vulnerable to various assaults, providing an authentication method between the source and destination nodes is crucial. How to route in such networks more efficiently, taking into account node mobility characteristics and accompanying massive historical data, is still a matter of discussion. Fuzzy logic-based Trusted Routing Protocol for vehicular cloud networks (FTRP) is proposed in this study that determines the secure path for data dissemination. Fuzzy Logic determines the node candidacy value and selects or rejects a path accordingly. The cloud assigns a confidence score to each vehicle based on the data it collects from nodes after each interaction. Our study identifies the secure path on the basis of trust along with factors such as speed, closeness to other nodes, signal strength and distance from the neighbouring nodes. Simulations of the novel protocol demonstrate that it can keep the packet delivery ratio high with little overhead and low delay. FTRP has significant implications for deploying Vehicular Cloud Networks using electric vehicle technologies in smart cities. The routing data is collected with the help of Internet of Technology (IOT) sensors. The information is transmitted between vehicles using IOT gateways.

KEYWORDS
fuzzy routing, smart cities, trust computation, vehicular cloud networks, vehicular cloud networks

1 | INTRODUCTION

Since vehicles now have precise locations, sophisticated computing/communication and enormous storage capacity (Onieva et al. 2019; Qu et al., 2015). Vehicular Ad Hoc Networks (VANETs) have truly become the dominant force in distributing and providing position-related data like route information. It improves road safety, reduces traffic accidents and congestion and prepares the way for more strategic travel planning (Onieva et al. 2019; Qu et al., 2015; Liang et al., 2019). The Intelligent Transportation System (ITS) is used by a variety of automakers including

Ferrari, Land Rover, Mercedes-Benz, Tesla, BMW, Volvo, Audi, and Ford among others, to deliver services to passengers and drivers (Hafeez et al., 2013; Karagiannis, 2011; Shen et al., 2011; Sichitiu & Kihl, 2008; Zeadally et al., 2012). These services improve the quality of driving and cut down the number of accidents on the road. Vehicles in a vehicular ad hoc network often use wireless transceivers to communicate with one another in a vehicle-to-vehicle (V2V) mode and with infrastructure. The ability of drivers to make decisions can be improved from the transmission of information in real time about their intentions for the road. Emergency vehicles may move over to allow other vehicles to use their lane in an emergency. When roads are backed up, the traffic monitoring system may send alerts and drivers may modify their routes. One of the most critical tasks in the VANET study is data distribution which relies heavily on reliable routing protocols (Yang et al., 2016). Specific limitations such as reducing-to-end time and packet loss during forwarding should be included in VANET routing protocols to accommodate the varied needs of traffic consumers. Until this, researchers have suggested routing protocols to guarantee steady data transfer and information exchange between vehicles; these protocols may be split into two groups (geography-based and topology-based) according to their respective networking approaches (Bitam et al., 2015). The VANET node's rapid and unpredictable movement constantly shifts the network's topology. Therefore, the position-based protocol is more effective for the VANET.

In addition, the difficulty of the routing protocol design is exacerbated by VANET's distinctive characteristics, such as its inherent instability, complexity and unpredictability. VANET is more prone to intrusion because of its features. Data loss may occur due to false messages, dropping of the packets or re-routing packets to the incorrect relay nodes done by malicious vehicles (Nagaraju et al, 2022). The driver may need to make better decisions based on harmful information obtained from misbehaving vehicles. If the data's trustworthiness cannot be effectively verified, it leads to massive traffic backups.

VANET is one existing model used in collaboration with other innovative technologies. To improve the Intelligent Transport System (ITS) and provide efficient data exchange with other vehicles, Internet of Vehicles (IoV) is developing a dynamic system of vehicles. Modifications in VANETs that exchange information with one another and with Road Side Units would be simple using IoV. The infrastructure of IoV is built around extending and improving the dependability of VANETs to boost travel services and driver awareness by keeping tabs on traffic conditions, in particular, to direct and prevent road accidents, find less congested routes, use less fuel, and produce less pollution (Zhang, Ge, et al., 2019; Zhang, Zhang, & Liu, 2019). Numerous cryptographic and trust-based security procedures (Chen et al., 2018; Li & Song, 2016; Yao et al., 2016; Yu et al., 2015; Yu et al., 2016; Zhang, Ge, et al., 2019; Zhang, Zhang, et al., 2019) have been offered as potential solutions to the routing security issue. However, trust-based security methods are commonly used to counteract assaults from inside (Li & Song, 2016; Yu et al., 2016, p. 15). Still, a significant difficulty in VANET is developing a trustworthy and effective routing protocol based on the trust paradigm, along with increased throughput, little overhead, and minimal end-to-end delay.

In this article, we first calculate the trust of every node in the network based on the trust offloading idea, in which the vehicles connect and provide the relevant statistics to the cloud to compute the trust using hybrid trust. Hybrid trust combines the current direct and indirect trust from the other nodes in the network. Using the IOV principle, vehicles can have direct conversations with the cloud or go via the RSUs without an internet connection. After every interaction, the interactive nodes calculate the stats based on provided services and send these stats to the cloud. Cloud calculates the trust and sends it to a node that demands any future node's trust. Using fuzzy Logic, a trustworthy routing method is developed. To select the next relay node or link/path, fuzzy Logic uses the node's trust value from the cloud. Suppose if the trust is greater than the predefined threshold value, then the other parameters of that node are also considered, like speed, link quality, number of neighbouring nodes, and distance to calculate the node candidacy value. This value of candidacy determines whether the link or path will be accepted or rejected. A comparison of the proposed routing protocol results with existing methods regarding packet delivery ratio, latency, and throughput has been performed.

This paper's remaining sections will be laid out as follows. Recent literary works are discussed in Section 2. In Section 3, the application scenario is discussed. Section 4 elaborates routing model process in depth. We propose a fuzzy logic for the routing mechanism in Section 5. Section 6 displays the outcomes of the experiments. The last section provides some final thoughts and suggestions for further study.

2 | LITERATURE SURVEY

The dynamic nature of nodes in a VANET makes routing challenging (Fadlullah et al., 2010; Li et al., 2007, 2012, 2014; Marwaha et al. 2004; Meng et al., 2016; Xiang et al., 2011; Xu et al., 2015; Yen et al. 2011; Youssef et al., 2014; Zeng et al., 2013). Many effective position-based routing techniques exist in VANET for transmitting data to its intended vehicle (Li et al., 2007; Zeadally et al., 2012). Despite transmitting data along the shortest path possible, present routing techniques generate significant delays in data forwarding because they create network gaps between vehicles along the route. End-to-end delays are minimized with cloud computing since fewer routes need to be taken. Internet connectivity decreases the need for vehicles to communicate over many hops, reducing the number of roadways required for transportation. Routing protocols in VANET using cloud and fuzzy Logic are explored below.

To effectively transmit data to the intended vehicle, RVCloud Bhoi and Khilar (2016) suggested a routing protocol for VANET to use cloud computing. Vehicles transmit beacon data to the cloud through RSU. With limited onboard memory and processing power, the city's network of moving vehicles relies on the cloud to store and manage their data. Information is sent from the source vehicle to the receiver through the nearest

RSU. The RSU then requests from the cloud the optimum RSU information needed to deliver the data with the least possible delay. The cloud-based solution gives the optimum RSU information and the final destination. The data is then sent through the internet from the RSU to the best RSU. Using the internet's infrastructure reduces the impact of issues like packet forwarding latency and connection interruption. But security is a significant factor in VANET and should be considered in this study as VANET is open to all and more vulnerable to attacks by malicious nodes.

A routing system, VehiCloud Qin et al. (2012), employs cloud computing to expedite data transfer. Every RSU and some of the city's vehicles are connected to the internet. The number of RSUs available in the metro area is low. By transmitting data to other vehicles and RSUs with internet access, vehicles upload details about themselves, including their identities, locations, and speeds, to a central server in the cloud. When a source needs to transmit information to a receiver, it requests the cloud, which determines the most efficient route to take and prioritizes those routes that pass via internet-enabled vehicles and RSUs. The cloud constructs a Time Space Link Graph (TSLG) and transmits it to the desired vehicle. The data is then sent following the route. Traditional routing procedures are used to transmit the data to the target vehicle if the RSU is far away, which increases the packet forwarding latency due to network gap encounters.

For entirely unexpected VANET, Shen et al. (2017) suggested the Trustworthiness Evaluation-based Routing protocol (TERP). To determine which nodes in a list of potential relays should be chosen, this protocol has the cloud server compute a trust score for the nodes on the list. The cloud server calculates the trust between nodes based on the parameters the nodes send to the server. In addition, vehicles in the network choose trustworthy forward nodes and finish the whole route based on the cloud's reliability. Packet delivery ratio, normalized routing overhead and average end-to-end latency are all areas where this protocol excels in simulation from other schemes, as the trust is calculated by the cloud based on parameters that nodes provide themselves. The malicious nodes may send false information of their own to the cloud. Therefore, the chances of false trust calculation increase.

Three steps were presented by a fuzzy logic-based routing approach by Azhdari et al. (2022) for vehicular ad hoc networks, including clustering, routing between cluster head nodes, and authentication. Vehicles are grouped in the first stage utilizing an effective method. The route-finding procedure for transmitting the instant and regular packets is added in the second phase. The last stage's goal is to guarantee data security. Each vehicle must perform an authentication procedure to confirm the legitimacy of the sender node before it can begin to receive data packets. Simple and secure data paths are introduced in this approach. Secure data packets use a message authentication code (MAC) and symmetric key cryptography-based authentication system. There is no authentication method for simple data packets. There needs to be a robust communication security system. SUMO traffic generators can be employed to create various vehicle speeds.

A trust-based architecture by Rostamzadeh et al. (2015) is suggested for the secure and trustworthy broadcast of information in vehicle networks. The first component of this architecture performs three tests to validate the message's authenticity. Instead of assigning a trust value to each vehicle, it does it to the route or neighbourhood. As a result, it is entirely distributed and has a high capacity for scaling. After determining whether a message is trusted, the second module seeks a secure channel. These frameworks may meet each application's unique traffic needs due to an application-centric approach. This framework outperforms popular routing protocols in experiments because it delivers messages via a verified route. Distributed trust management approach is used in this paper. Vehicles must maintain the trust table for each area, which may generate overhead for each vehicle.

Using software-defined vehicular ad hoc networks (SD-VANETs) Vasudev and Das (2018), networks may be made more manageable and flexible via programming. Additionally, the author focused on recent recommendations meant to improve the security and routing of SD-VANETs in an organized and architectural fashion. In a dynamic setting, this system uses a trust-based notion to identify malevolent vehicles while decreasing overhead by ignoring vehicles with a trust value of 0 and providing two algorithms to do this. This study demonstrated that detecting rogue vehicles in SD-VANETs is an NP-complete issue. According to the Trust-based algorithm, the RSU shall validate each on-road vehicle based on the vehicle's Digital Licence Plate (DLP) before starting communication. If accurate, the Trust Value (TV) is set to 1, allowing the vehicle to participate in communication; otherwise, the Trust value is set to 0. This approach only authenticates the vehicle. Once the vehicle is authenticated, it can send bogus messages later to harm the network. So, there is a need for an approach that identifies such nodes in the network with the time.

The Dissemination Protocol uses a cloud computing architecture for VANET (ClouDiV) Bitam and Mellouk (2015) allow adaptive dissemination of safety and non-safety signals. ClouDiV combines a flexible cloud structure based on onboard vehicles' computers with a fixed cloud computing infrastructure (i.e., data centers). Each data Centre is suggested to take a proactive approach while using ClouDiV, a hybrid message distribution protocol, to find new and updated routes to every network node. There is no security measure used to authenticate the nodes (Nittu et al, 2023). The use of proactive and reactive approaches may increase the delay.

A fuzzy trust model by Soleymani et al. (2017) that counts experience and plausibility is introduced for providing a secure vehicular network. This model applies various security checks to ensure the integrity of the information received from the vehicle. Fog nodes are used to evaluate the accuracy level for the event's location. The paper aims to detect the various malicious attackers and nodes and reduce the uncertainty and imprecision of data in both environments, like line of sight and non-line of sight. According to the author, using the Fuzzy Logic event's location, the event's location is fetched if it is available in the closest Fog node, which needs to be mentioned. If the event is not available on the fog node, then how does the location of the event parameter serve its purpose of evaluating the trust value?

To compute the communication security in VANET, a fuzzy Logic-based scheme by Igried et al. (2022) is used to detect the malicious nodes and improve the utilization of the resources in the Vanet. The node with the lower trust level (TL) cannot participate in the communication. This scheme uses the public key cryptography technique for authentication. The concerned RSU decides the road status based on data from the different nodes and their TL values. Emulation attack attempt, collaboration degree and RSU assessment are the factors used to compute a node's trust level in the network. Based on complicated mathematics, public key encryption may result in a computational overhead that may delay more.

Further, it only checks the node's authentication but can't prevent the authenticated node from sending bogus messages. RSU is completely reliable on the data transmitted by the nodes so that the few malicious nodes can send the bogus information in collaboration with RSU. Result evaluation of this scheme is done with another scheme using the matrix like end-to-end delay, packet delivery ratio, and packet loss ratio.

3 | EXPERIMENTATION SCENARIO

It is a challenging task to identify the next-hop neighbour node in VANETs because of the properties of the network and the fact that it is a very dynamic system. We chose the best possible next-hop neighbour node for VANETs by considering many different characteristics. Many security measures and how the fuzzy logic helps to identify the secure path by considering the different parameters have been discussed in this section.

3.1 | Security threats

Vehicles in the network can participate in various malicious activities such as false reporting, conspiring with another adversary vehicle, on-off attacks, and sending bogus messages to other vehicles in the network. These malevolent behaviours can be mixed to create dynamic malicious models. In False Reporting Each vehicle reports the Quality parameters of another vehicle to the cloud after communicating with it. Adversary vehicles report bad QOS parameters to the cloud to lower their trust value and gain an advantage. Connive with other Adversary vehicles is a potent attack where one adversary vehicle praises its partner (another adversary vehicle) by reporting its QOS parameter above the average and distracts the other trusted vehicles. In this way, the trusted vehicles trust the malicious vehicles. Adversary vehicles have more opportunities to deliver network services or, in other words, have more chances to damage the network. Adversary vehicles in an On-Off Attack often act as trusted vehicles, providing good network services, and other times, they act as adversary entities, providing bad services to interrupt the network. These vehicles are relatively easy to spot. VANET safety information contains sensitive data critical for the smooth operation of the network and the safety of drivers, etc. Adversary vehicles may inject forged Information into the network about route congestion or causing route diverting.

3.2 | Why fuzzy logic?

The application scenario of this paper can be described as follows: if vehicle A wants to communicate with another vehicle B in the network, then communication must be done through a secure path that considers the trusted vehicles with high candidacy values. If the two vehicles communicate, vehicles A and B will send the QOS parameters of each other to the cloud, which will be used to assess and update the vehicles' trust. Fuzzy Logic is used to deal with uncertainty. Fuzzy combines the different parameters and makes the rules according to them. The primary parameter is trust; if the node is trusted, other parameters are also considered; otherwise, the node is rejected. The integration of parameters like trust, speed, distance, number of neighbouring nodes, and signal strength decide the candidacy value of the node. If it is high, the path is accepted, and the node is considered the next relay node to send the message further. Considering Crisp values for parameters like distance, speed, signal strength, and number of neighbouring nodes needs to be improved. So here, fuzzy Logic aims to define the ranges for such parameters and make rules accordingly to provide the most robust, trusted path among the others. Each parameter has its importance, like trust—It initially filters the malicious nodes and discards the node, eliminating the need to consider further parameters. Distance affects the signal's strength and time to exchange the data. Number of neighbouring nodes—a large number of nodes provides the maximum chances to communicate with the non-malicious nodes in the network. Speed—if the vehicle's speed is very fast, they have a very short time communicating with nodes. If the normal-speed vehicle is available near the transmitted vehicle, the next relay node will be that instead of a high-speed vehicle. Link Quality—it should be good to transmit the message or data as it reduces the chances of breaking the signal.

4 | FUZZY-BASED TRUSTED ROUTING PROTOCOL (FTRP) PROCESS

We employ a mechanism known as the Fuzzy Logic-based Trusted Routing Protocol (FTRP) to select the next forwarding node in the chain. The suggested next-hop forwarding nodes can forward packets reliably while maintaining high efficiency. The choice of the next-hop node in a routing algorithm is determined by several different metrics about the vehicles involved, including their speed and inter-vehicle distance, Link quality, nearby Nodes, and Trust. The trust parameter is crucial since it is the standard or default value. A node's candidacy value is lowered, and the route is denied if the node's trust does not meet a specified minimum value. If a particular node's trust is more than 0.5, additional criteria are used to determine the node's candidacy value.

Furthermore, the trust of a node is not computed locally at the node itself. Following each interaction, vehicles upload the stats to the cloud that they have gathered about the quality of service provided by other vehicles. After that, the direct statistics and the history of trust are used on the cloud to determine the hybrid or combined trust of the vehicles. This reduces the probability of erroneous trust calculations.

Figure 1 shows how FTRP operates to find out the node candidacy value. Trust is used as the standard parameter and the four additional parameters. The trust parameter has an impact and acts as an input to FIS if its value is more than 0.5, in addition to the speed, link quality, IVD, and nearby nodes. The FIS output is the value of a node's candidacy. If the node's candidacy value is more significant than 0.75, the route will be approved; otherwise, it will be rejected. Similarly, Algorithm 1 shows the step-by-step path selection procedure for requesting node Q and target node T.

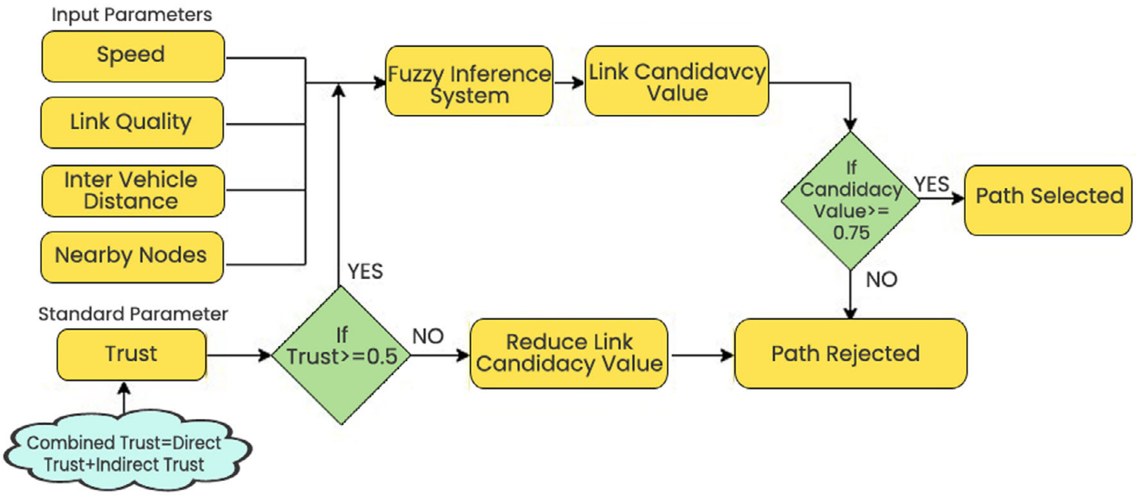

FIGURE 1 Fuzzy Logic-based Trusted Routing Protocol process.

ALGORITHM 1 **Path Selection from Requesting Node Q to the target Node T**

```
T ← Target Node
    P ← empty set of relay paths (entries to next hops)
    C ← current Node (Q)
    N ← all nodes in the range of the current node C
    FIS ← Fuzzy Rule based on an Inference system using speed, IVD, link quality, nearby nodes, and combined trust.
    While T is not in N
    for each candidate node c in N
    Estimate node speed, IVD, link quality, nearby nodes & Fetch combined trust from the cloud of each node c in N
    Node Candidacy = FIS (speed, IVD, link quality, nearby nodes, combined trust)
    If Node Candidacy < 0.75
    Continue;
    Else
    Push candidate node c in P End
    End
    End
    N ← gets all nodes in the range of the current node C sorted by their candidacy value such that the highest-scoring node is at
the top.
    End for
    End while
    Return P
```

5 | FUZZY LOGIC FOR FTRP

Due to problems with completeness, unpredictability, and data loss, scientists have concluded that real and complex processes are impossible to measure, model, or regulate Pham (2020). Fuzzy sets are characterized by their partial membership, which includes results that are mostly true or mostly false rather than totally true or completely false. The four main parts of a fuzzy system are fuzzification (the transformation of discrete data into a fuzzy value), the rule base (a set of if-then rules), the fuzzy inference engine (which generates a nonlinear map between input and output), and defuzzification (to convert the fuzzy value to the crisp value). Combining fuzzy rules in various fuzzy systems may be done in several ways, each with its concepts and procedures. The two most influential forms of fuzzy inference are Mamdani fuzzy inference and Sugeno fuzzy inference. In this study, we used the Sugeno fuzzy Inference model, which takes five membership functions as input and generates outputs as a value for the node's Candidacy value f(u). The dependability of a node is defined by its node's candidacy value, which indicates the degree to which that node is nominated to deliver services inside the network.

$$f(u) = \{S_{\mathrm{d}}, L_{\mathrm{q}}, N_{\mathrm{i}}, IVD, \Psi_{\mathrm{i}}\}. \tag{1}$$

A vehicle's speed (S_d) is specified by the membership function speed, nearby nodes (N_i) of an ith node are indicated by the nodes nearby membership function, inter-vehicle distance (IVD) indicates a distance between vehicles of roughly 250 meters, combined trust of node (Ψ_i) indicates a node's reliability as calculated from its direct and indirect trust values, and link quality specifies the strength of the signal.

5.1 | Input parameters calculation and representation of membership functions

During the span of the simulation, the values for speed (S_{d}), near nodes (N_i), inter-vehicle distance (IVD), and link quality (L_{q}) are all calculated in real-time. The Gaussian MF block is used to implement the membership functions.

$$f(\mathrm{q}; \sigma_i, \times_i) = e^{\frac{-(q-\times_i)^2}{2\sigma_i{}^2}}, \tag{2}$$

where $i = 1, 2$, the curve on the left is defined by the mean and standard deviation, respectively denoted by the values $\times_1$and σ_1. The mean and standard deviation that define the curve on the right are represented by the parameters $\times_2$ and σ_2, respectively.

5.1.1 | Calculation of vehicle's speed

Due to the highly dynamic nature of vehicular nodes in VANETs, speed is a crucial parameter to monitor. Speed is calculated by the total distance covered in a particular time stamp divided by the time taken. The average speed of the vehicle is calculated by Equation (3).

$$S_{\mathrm{d}} = \sum\nolimits_{t=0}^{n} \frac{\sqrt{(\mathrm{x}_2 - \mathrm{x}_1)^2 + (\mathrm{y}_2 - \mathrm{y}_1)^2}}{\mathrm{t}}. \tag{3}$$

We divided the speed into three distinct classes: the low category is from 0 to 25Km/h, the mid-range is from 25 to 75 Km/h, and the high range is from 75 to 100 Km/h. The membership functions for the speed mentioned above classes are described and shown in Figure 2.

5.1.2 | Calculation of link quality

Link Quality specifies the strength of the signal, and it is determined by the Received Signal Strength (RSSI) after normalization, as shown below.

$$\text{Link Quality}\,(Lq_i) = \frac{(R_{i-}\min(R))}{(\max(R) - \min(R))} \tag{4}$$

Here, the Link quality Lq of the ith data value is a normalized value between 0 and 1 of the RSSI ith value (R_{i}). Figure 3 provides a representation of the membership function of link quality, where if the link quality value is below 0.3, then it is considered to be bad; if it is between 0.3 and 0.8, then it is considered to be normal; and if it is above 08, then it is considered to be excellent.

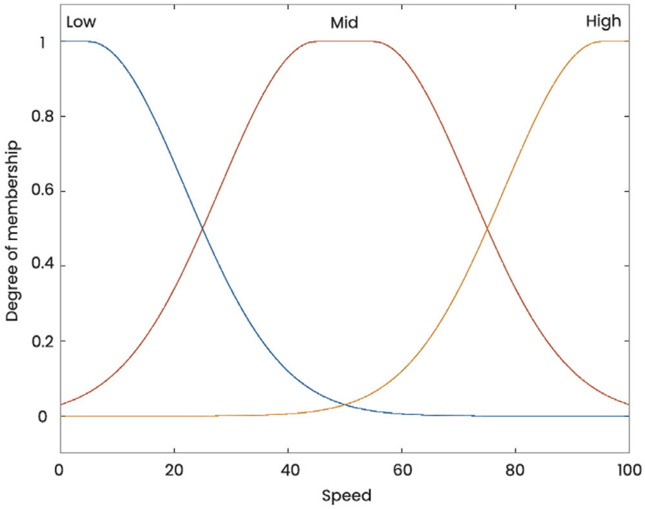

FIGURE 2 Graphical representation of speed metric.

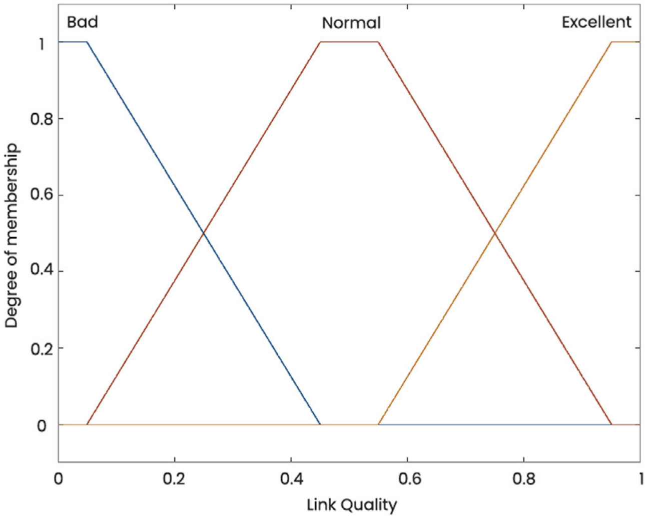

FIGURE 3 Graphical representation of link quality metric.

5.1.3 | Calculation of trust

In this study, trust is calculated using the concept of Trust of flooding (Kaur, 2022), which combines direct observations with neighbouring node suggestions to compute the final trust value of a node in the network. Every vehicle in the network evaluates the functions of a node with which it has interacted and computes statistics. These statistics are subsequently used to determine the vehicle's trustworthiness. The nodes' packet forwarding and routing ratios determine direct trust. The number of packets that do not transmitted divided by the total number of forwarded packets is directly related to the malicious propensity of the node, which is first detected before computing the direct trust. The malicious propensity of node *P* is calculated using the following equation.

$$D(T)_p^q = \sum_t^T \frac{\omega(t)}{\sum_1^n \omega(t)} \times M(t)_p^q, \tag{5}$$

In this case, $D(T)_p^q$, known as direct trust, provides a mean trust value and a confidence interval around the mean. The estimated statistics for node *q* are denoted by $M(t)_p^q$ and calculated by node p using the statistical behaviour of node *q* at time *t*. Calculated by the number of packets that are not transmitted divided by the total number of forwarded packets is directly related to the malicious propensity of the node.

$$M(t)_p^q = \frac{\left(T(P)_p^q - S(P)_p^q\right)}{\left(T(P)_p^q\right)}. \tag{6}$$

To prevent biased trust and promote impartiality, third-party input is crucial. It is crucial to measure it using several neighbours' viewpoints since it is significantly impacted by the presence of recommendations from a third party $\left(R_n^q\right)$.

$$R_n^q = \frac{\sum_{i=1}^{N} \Psi_i \times D(T)_p^q}{\sum_{i=1}^{N} \Psi_i}. \tag{7}$$

To improve the reliability of recommendations, it is essential to use direct and combined trust from n neighbours. Since there may be many other nodes within the range of node *q*, we have restricted our selection to those that have established direct trust *D*(*T*) from node *p* to node *q*.

The Combined Trust is the sum of both direct trust and recommendations. The key issue is figuring out what to do with their various stakes. The degree of direct trust between two nodes may vary depending on their history of connections. Furthermore, in multiple contexts, the power of a suggestion may significantly increase or decrease trust. Based on data, a dynamic balancing coefficient in [0,1] regulates trust effects. The combined trust (Ψ) of node *q* by node p is calculated as:

$$\Psi_p^q = \tau.D(T)_p^q + (1-\tau).R_n^q. \tag{8}$$

In Figure 4, two linguistic variables define the trust matrices. If the trust level of the node is less than 0.5, the vehicle is considered a potentially malicious entity. On the other hand, if the trust level is more than 0.5, the vehicle is regarded as a trusted entity.

5.1.4 | Calculation of inter-vehicle distance (IVD)

The acronym 'inter-vehicle distance' (IVD) refers to the distance, in meters, that may exist between two vehicles. This distance cannot exceed 250 m. The membership function of IVD, as shown in Figure 5, used three linguistic variables: close, reachable, and Far. If the distance between a vehicle and its neighbouring node is less than 100 meters, the distance between the vehicles is considered the closest. If the distance is between 100 and 150 m, it is assumed that the vehicle is reachable; however, if it is more significant than 250 m, the vehicle is considered far.

5.1.5 | Nearby nodes calculation

The number of nodes adjacent to node i is measured by the nearby nodes (N_i) metric. N_i's values may be represented by the terms 'low', 'mid', and 'high'.

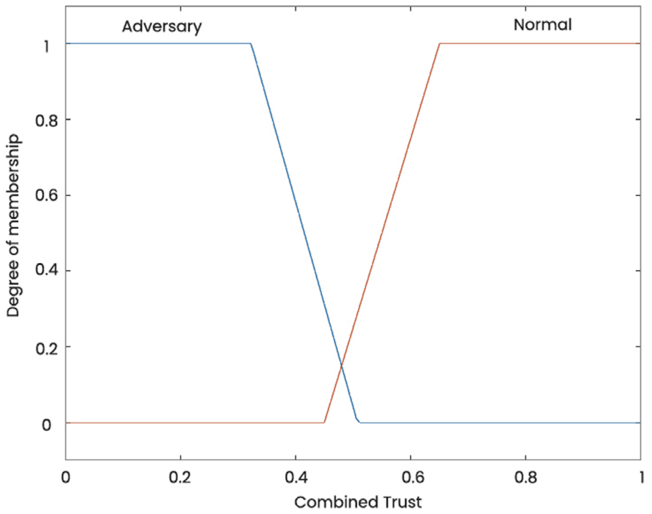

FIGURE 4 Graphical representation of trust metric.

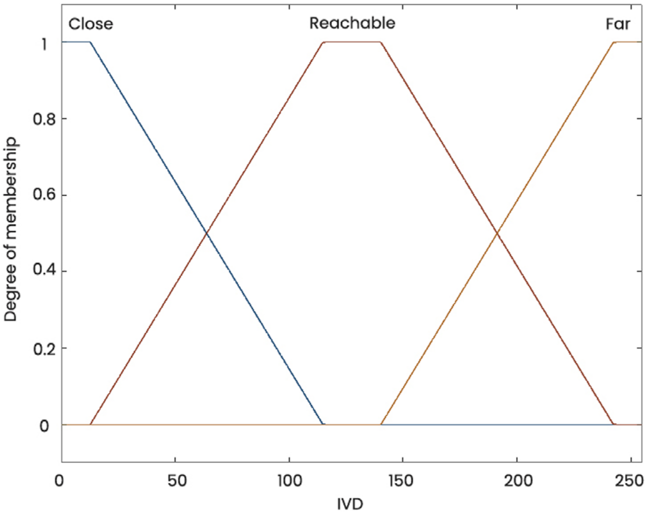

FIGURE 5 Graphical representation of inter-vehicle distance metric.

If there are less than three nodes in the immediate area, it indicates a sparse vehicle population; between three and seven nodes indicates a moderate vehicle population; and more than seven nodes indicate a dense vehicle population.

5.2 | Output variable

The result displays the characteristics of routing metrics, which determine which node offers the most advantageous next-hop for routing. The Gaussian MF establishes the output node candidacy value from 0 to 1. Consequently, the output variable is separated into two categories: path selected and path rejected. If the value of the node candidacy is more significant than 0.75, then the adjacent node will be chosen. The following equations are used by gauss2mf to get the output:

$$\mathrm{F}(\mathrm{x})\mathrm{Path}_{\mathrm{Selected}} = \begin{cases} 0\,(x < 0\,or\,x > 1) \\ . \\ \dfrac{(x-1)^2}{e^{\sigma_i{}^2}}(0 \le x \ge 1) \end{cases}, \tag{9}$$

$$\mathrm{F}(\mathrm{x})\mathrm{Path}_{\mathrm{Rejected}} = \begin{cases} 0\,(x < 0\,or\,x > 1) \\ . \\ \dfrac{(x-0.75)^2}{e^{\sigma_i{}^2}}(0 \le x \ge 1) \end{cases}. \tag{10}$$

The graphical representation of the 'nearby nodes' metric is shown in Figure 6. The network nodes' spatial distribution and connectivity patterns are displayed visually. The metric measures how close or dense a node is to its neighbours for each node in the network. This display lets Users learn more about local connectivity features and find areas with more significant or lower concentrations of neighbouring nodes. With an emphasis on the spatial relationships between nodes, the graph provides a clear and understandable overview of the network topology.

5.3 | Fuzzy rules

Fuzzy IF-THEN rules represent the human knowledge in FIS. To link input and output variables, these rules use trusted routing protocol criteria that are fuzzy-based. If (fuzzy preposition), THEN (fuzzy preposition) is a fuzzy-based IF-THEN rule. The outcome or conclusion is THEN when the condition or premise is IF. For instance, the first condition in the table specifies that if the vehicle's speed is low, the connection quality is bad, there is a limited population of nearby nodes, and the IVD is close, the node Candidacy value is denied. The trust metric is essential, and if a node's Candidacy value suggests that it is malicious, a route will always be rejected. In addition, if trust is at a Normal level, the output relies on the other metrics. One hundred thirty-three different regulations could be implemented for this specific circumstance. Table 1 provides an overview of the

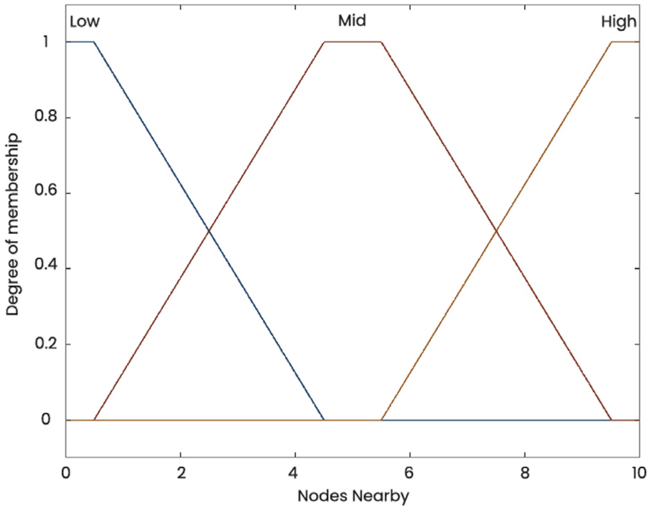

FIGURE 6 Representation of nearby nodes' metric.

TABLE 1 Fuzzy rules.

Rules	Speed	Link	Nearby	IVD	Trust	Node candidacy
Rule 1	Low	Quality Bad	Nodes Low	Close	Adversary	Value Rejected
Rule 2	Low	Bad	Mid	Far	Adversary	Rejected
Rule 3	Low	Normal	High	Close	Adversary	Rejected
Rule 4	Low	Excellent	Low	Close	Adversary	Rejected
Rule 5	Low	Excellent	Low	Reachable	Adversary	Rejected
Rule 6	Mid	Bad	Low	Reachable	Adversary	Rejected
Rule 7	Mid	Bad	High	Close	Adversary	Rejected
Rule 8	High	Bad	Low	Close	Normal	Rejected
Rule 9	Low	Bad	Low	Far	Normal	Rejected
Rule 10	Low	Bad	Low	Close	Normal	Rejected
Rule 11	Low	Normal	Low	Reachable	Normal	Selected
Rule 12	Low	Normal	Low	Far	Normal	Selected
Rule 13	Mid	Normal	Mid	Close	Normal	Selected
Rule 14	Mid	Normal	Mid	Reachable	Normal	Selected
Rule 15	Mid	Normal	Mid	Far	Normal	Selected
Rule 16	Mid	Excellent	Low	Close	Normal	Selected
Rule 17	High	Excellent	Mid	Close	Normal	Selected
Rule 18	High	Excellent	Mid	Far	Normal	Selected
Rule 19	High	Excellent	High	Far	Normal	Selected
Rule 20	High	Excellent	Low	Far	Normal	Selected

20 other rules that might be used instead. To accurately determine the Node Candidacy values of neighbouring nodes, the FTRP protocol considers a wide range of additional parameters besides the trust value. The speed between vehicles, the gearbox range, the connection quality, the number of neighbouring nodes, and the trust value are some of these characteristics. The three-dimensional graphics 7, 8, 9, and 10 provide a more in-depth look at the potential conclusions that may be obtained using fuzzy Logic. These three-dimensional graphs show how the input and output variables act in a correlational manner with one another and how that behaviour is displayed. Figure 7 presents a 3-D graph that illustrates how the value of the node Candidacy steadily increases when the value of the connection quality or signal strength improves, in addition to the number of nodes positioned in close proximity to one another.

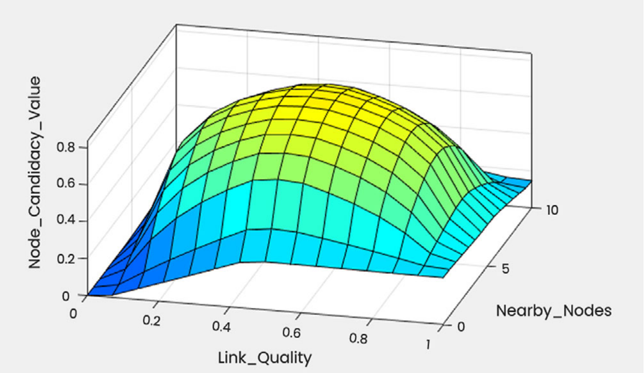

FIGURE 7 Node candidacy value for link quality and nearby nodes.

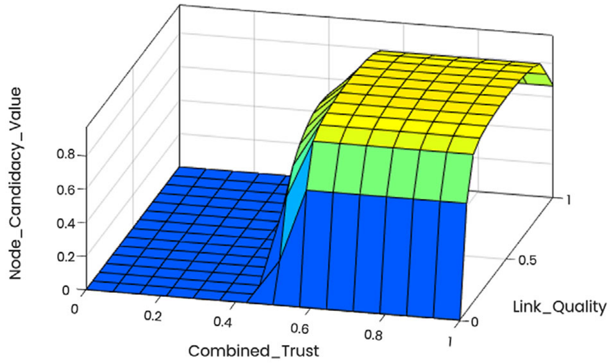

FIGURE 8 Node candidacy value for link quality and combined trust.

Figure 8 illustrates the pattern of the correlation between inputs such as combined trust and connection quality and the output referred to as the node Candidacy value. The value of a candidate node increases directly to the rate at which the trust and connection quality of neighbouring nodes that originate from the source grow. The degree of fuzziness produced due to this circumstance will likely be exceptionally high. This may be observed in the correlation three-dimensional graph, where the highest dark yellow portion highlights the correlation.

The correlation between close nodes, IVD, and output as node Candidacy value is shown in Figure 9. With more neighbouring nodes and closer distances between the Vehicle-less, node Candidacy increases.

The distribution of candidate values for speed and distance between vehicle is shown in Figure 10, which explains how the distribution looks. As can be seen in the figure, the candidate value increases when there is less space between the vehicles. This is something that should be taken into consideration. The FTRP has a higher node Candidacy value, which results in better outcomes when determining the lowest feasible distance that may be maintained between Vehicles.

6 | NETWORK PARAMETERS AND PERFORMANCE ANALYSIS

The MATLAB platform was selected to provide a simulation environment in which the FTRP protocol's performance could be compared to previously existing protocols. The MATLAB software package is a high-performance mathematical calculation, visualization, and programming tool. It's a versatile technical computing, graphics, and animation platform with hundreds of built-in features and a user-friendly interface. Using the SUMO movement model, simulated networks are constructed with nodes placed at random on a 1000 m × 1000 m grid. This section covers the performance assessments of the proposed FTRP according to its design in the presence of malicious vehicles in the network. TERP, Trust-based AODV (TAODV), and R2SCDT, three modern VANET protocols are compared with the proposed protocol (FTRP). The faster convergence of the routing algorithm is indicative of a low network communication overhead ratio. This is due to the fact that the phrase 'network routing overhead ratio' refers to the proportion of simulated packets used for routing as opposed to the overall number of simulated packets. Different parameters for simulation are given in Table 2.

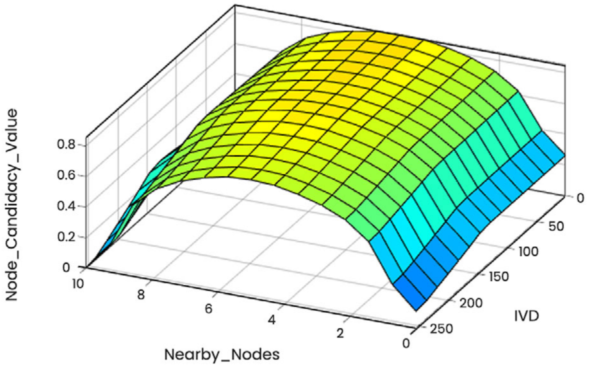

FIGURE 9 Node candidacy value for nearby nodes and inter-vehicle distance.

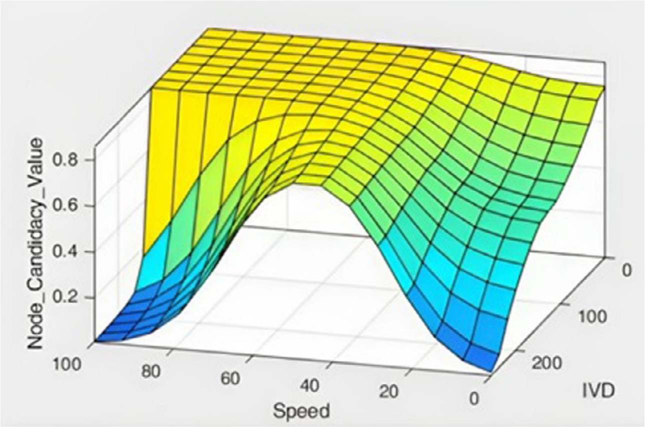

FIGURE 10 Node candidacy value for inter-vehicle distance at various speed of vehicle.

TABLE 2 Network parameters.

Parameters	Values
Node density simulation	[50–150]
Time	300 s
Mobility range (Km/h)	[10–70] (Azhdari et al., 2022; Bhoi & Khilar, 2016; Bitam et al., 2015; Bitam & Mellouk, 2015; Chen et al., 2018; Fadlullah et al., 2010; Igried et al., 2022; Kaur, 2022; Li & Song, 2016; Li et al., 2007, 2012, 2014; Marwaha et al., 2004; Meng et al., 2016; Pham, 2020; Qin et al., 2012; Rostamzadeh et al., 2015; Shen et al., 2017; Soleymani et al., 2017; Yang & Wang, 2015; Yao et al., 2016; Yen et al., 2011; Youssef et al., 2014; Xiang et al., 2011; Xu et al., 2015; Yu et al., 2016, 2015; Vasudev & Das, 2018; Zhang, Ge, et al., 2019; Zhang, Zhang, et al., 2019; Zeng et al., 2013)
Routing protocols	TERP, TAODV, R2SCDT, PROPOSED (FTRP)
MAC	802.11p
Mobility model	SUMO
Antenna	Omni directional
Traffic model	VBR
Number of adversary nodes	10%
Cloud trust storage	MySQL
Engine trust range	[0,1]
Monitoring area	1000 × 1000 m
Communication range	250 m

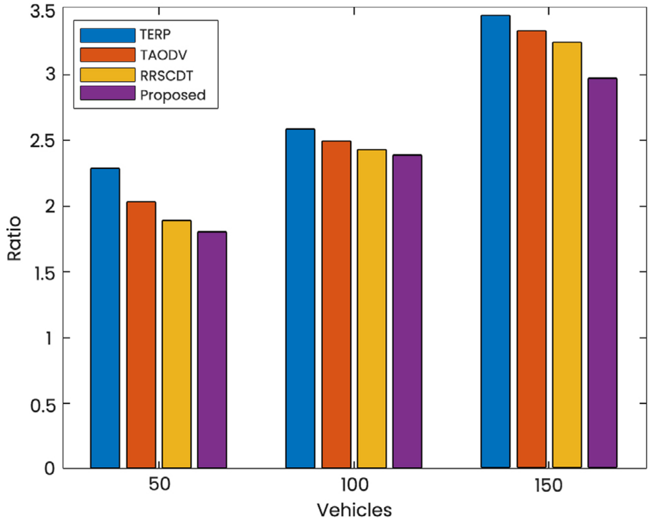

FIGURE 11 Communication overhead.

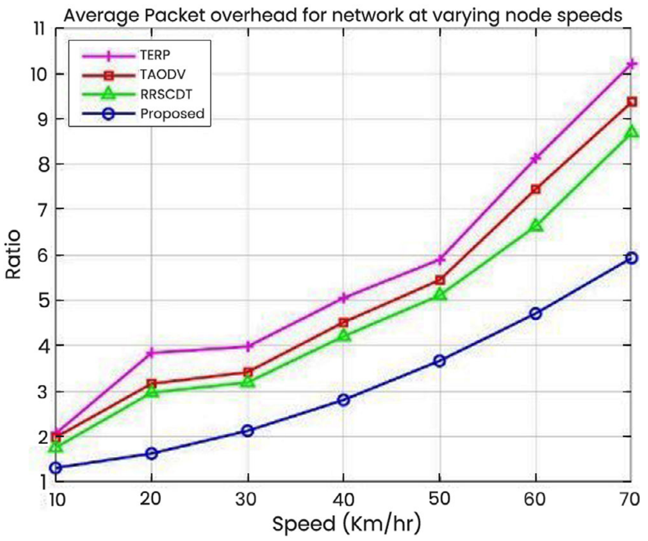

FIGURE 12 Communication overhead at vehicle speeds.

In Figure 11, we can see how the general communication overhead is steadily reduced over time. The proposed FTRP protocol has a lower overhead than competing protocols like TERP, TAODV, and RRSCDT. It shows that FTRP protocol has 0.13%, 0.23%, and 0.38% lower communication overhead than competing protocols RRSCDT, TAODV, and TERP, respectively. Figure 12 depicts the communication burden at the travelling speed of a vehicle. As the vehicle's speed grew, it may have resulted in communication breaks or incompleteness of transactions, increasing the communication overhead. Yet, FTRP still managed to function effectively with little overhead as compared to other protocols. Additionally, FTRP gives the preference to the trustworthy nodes. This is because the overhead rises if the route is broken after it has been constructed, and happens due to malicious nodes. The speed of a vehicle and the quality of the link are two additional key aspects that must be taken into account to reduce the time lost due to faults in the communication path. Vehicles travelling at a medium speed with high-quality links are given precedence in our work.

The communication overhead of several routing protocols, a proposed protocol, TERP, TAODV, and RRSCDT across a range of node scenarios is compared in Table 3. The values in the table represent the communication overhead metrics for each protocol for various node counts (50, 100, and 150). Lower communication overhead levels are generally better since they show more effective resource and data usage. The Proposed protocol is noteworthy for its consistently lower communication overhead than TERP, TAODV, and RRSCDT in all node scenarios. This suggests that the protocol effectively decreases communication overhead, mainly as the network grows with more nodes.

TABLE 3 Comparison of communication overhead.

Nodes	TERP	TAODV	RRSCDT	Proposed
50	2.2848	2.0273	1.8911	1.8085
100	2.5838	2.5011	2.4376	2.3889
150	3.4457	3.3289	3.251	2.9693

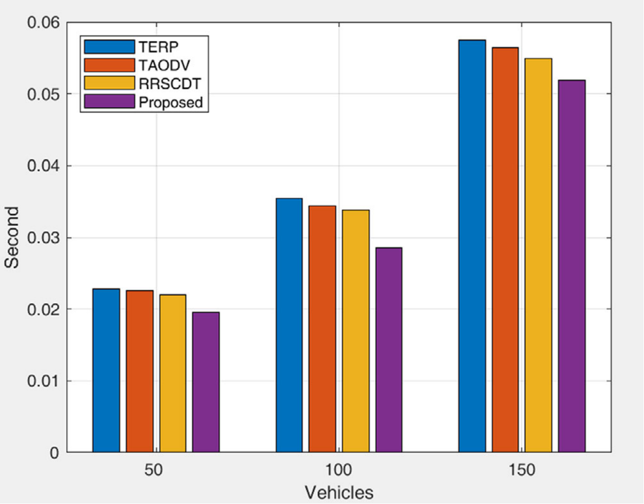

FIGURE 13 Average delay.

TABLE 4 Comparison of average delay.

Nodes	TERP	TAODV	RRSCDT	Proposed
50	0.022826	0.022609	0.021957	0.019529
100	0.035435	0.034348	0.033804	0.02748
150	0.0575	0.056413	0.054891	0.05192

The average delay is the same as the mean value of the instantaneous packet delays accumulated over a significant amount of time. The average delay increased gradually with the number of vehicles increased in Figure 13. The delay in seconds is determined as shown in Table 4. FTRP is 0.003% better than RRSCDT, 0.014% better than TAODV, and 0.005% better than TERP. The delay in FTRP is smaller as compared to other protocols. Vehicles' candidacy value increases if the node is trustworthy and achieves the specific range of parameters like speed and link quality. With increased vehicle speed, there is a risk of connection failure before communication is completed.

The average delay metrics for several routing protocols—TERP, TAODV, RRSCDT, and a Proposed protocol—across several node scenarios are compared in Table 4. The average delay in seconds for each protocol at various node counts (50, 100, and 150) is indicated by the values in the table. Lower average delay values are preferable since they indicate lower latency and faster data delivery. Analysing the data, it can be shown that in all node scenarios, the Proposed protocol continuously means a lower average delay than TERP, TAODV, and RRSCDT. To be more precise, the Proposed protocol's average latency at 50 nodes is 0.019529 seconds, demonstrating how effective it is at reducing transmission delays. As the network grows, this pattern continues, showing how well the suggested protocol works to minimize average latency in communication scenarios with varying node densities.

With increased vehicle speed, the average delay grew steadily in Figure 14. FTRP has a shorter delay than TERP, TAODV, and RRSCDT. The delay difference between FTRP and other protocols is more significant in dense populations of vehicles since high-trusted vehicles are taken into account.

The rate at which packets are lost in travel indicates how reliable a communication network route is. This measure is calculated by dividing the total number of packets transmitted and dividing that by the number of packets not received. It is clear from Figures 15 and 16 that FTRP has a lower average loss of packets compared to other protocols, which holds true value regardless of the number of vehicles or the speed of the vehicles. The packets were dropped by a malicious node, which is also responsible for the loss. The primary goal of this study is to limit communication to trustworthy nodes. Trust is calculated on the cloud rather than by individual nodes to accomplish this purpose. It decreases the

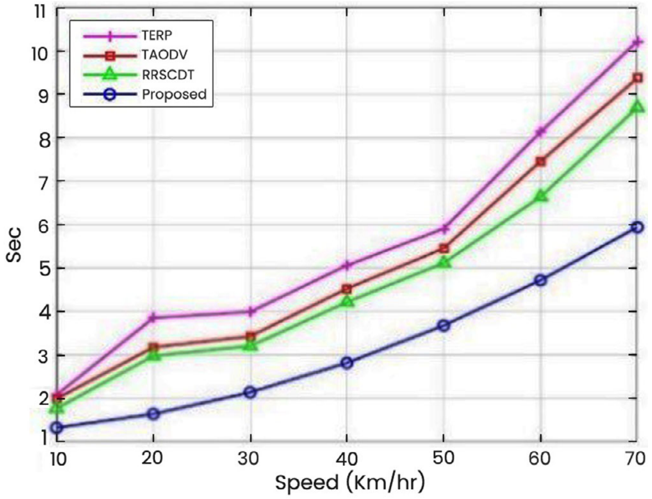

FIGURE 14 Average delay at node speed.

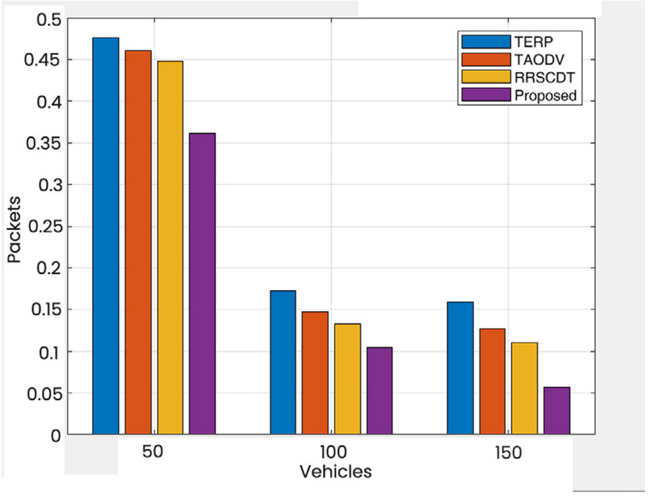

FIGURE 15 Average loss for network.

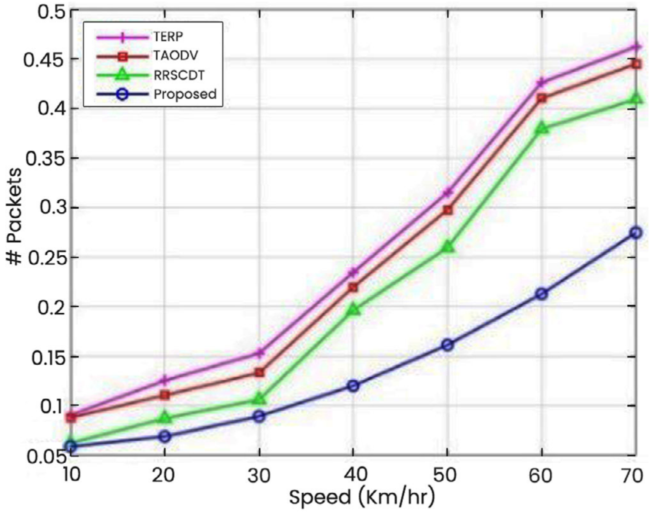

FIGURE 16 Average loss rate at node speeds.

TABLE 5 Comparison of average packet loss rate.

Nodes	TERP	TAODV	RRSCDT	Proposed
50	0.47572	0.46069	0.44798	0.36108
100	0.17283	0.1474	0.13237	0.10453
150	0.15896	0.12659	0.1104	0.057033

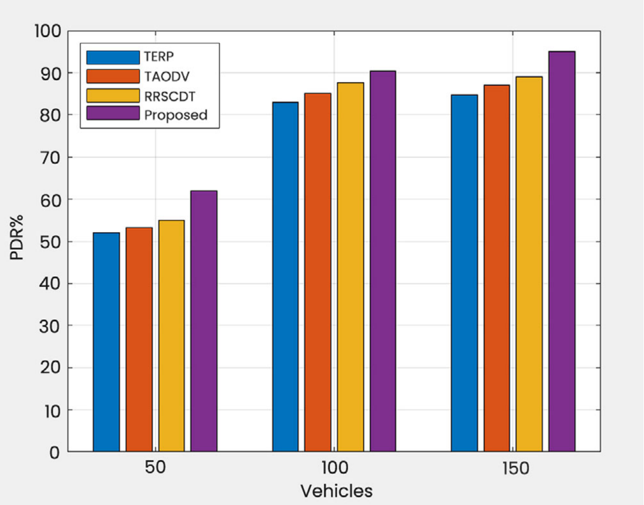

FIGURE 17 Average PDR for network.

TABLE 6 Comparison of average PDR.

Nodes	TERP	TAODV	RRSCDT	Proposed
50	52.13	53.199	55.01	61.913
100	83.043	85.068	87.727	90.277
150	84.78	87.121	89.039	95.09

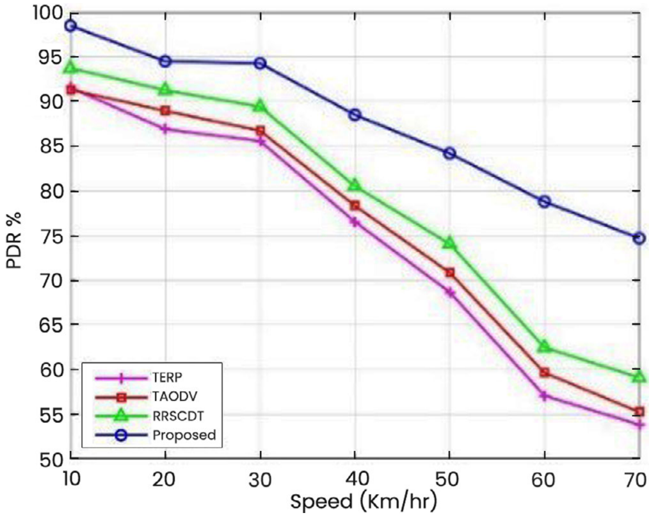

FIGURE 18 Average PDR at varying node speeds.

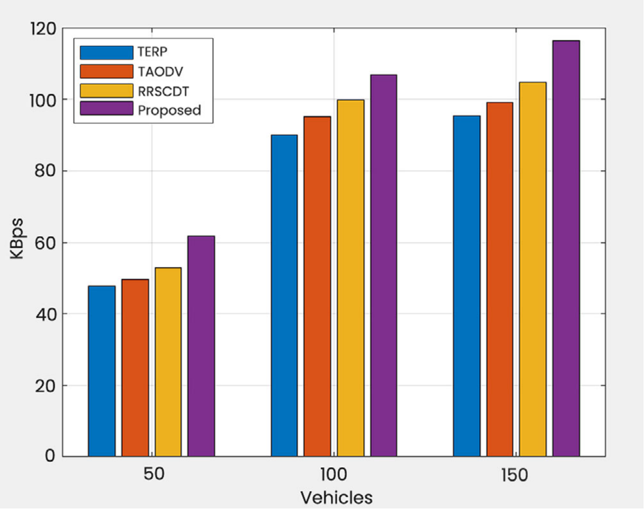

FIGURE 19 Average throughput for network.

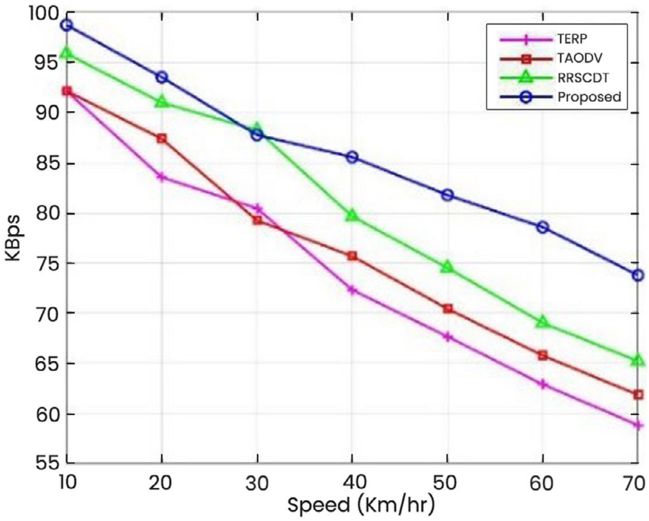

FIGURE 20 Average throughput at node speeds.

TABLE 7 Comparison of average throughput.

Nodes	TERP	TAODV	RRSCDT	Proposed
50	47.63	49.6	52.806	61.818
100	90.004	95.153	99.773	106.89
150	95.256	99.17	104.68	116.33

possibility of a bogus trust computation. Trusted nodes with strong signal strength are preferred for communication. Table 5 illustrates the average packet loss rate for the number of nodes. The suggested method has a lower average loss rate of 0.05%, 0.07%, and 0.09% than RRSCDT, TAODV, and TERP, respectively.

The proportion of data packets received by the destination node relative to the total number of data packets transmitted is known as the packet delivery ratio of a network. Figure 17 and Table 6 depict the effect of the number of vehicles on the PDR. FTRP outperforms RRSCDT, TAODV, and TERP by 5.1%, 7.2%, and 9.1% respectively.

Figure 18 illustrates the effect that speed has on the PDR. The procedure that was suggested, on the other hand, works effectively both when there are many vehicles and when there are few. This research does not accept links with high speeds since they pose a lower risk of connection failure.

The throughput achieved with FTRP is superior to that achieved with other protocols because of its high-quality link, shortest inter-vehicle distance, and speed. When compared to distance and speed, the importance of link quality is prioritized higher. According to Figures 19 and 20, the throughput of FTRP is higher than that of other protocols when considering the number of vehicles and the speed at which they move.

Table 7 shows the proposed (FTRP) scheme provides better throughput at varying nodes. It can be observed that FTRP performed 9.01 % better than RRSCDT, 12.21% more than TAODV, and 17.38% better than TERP.

7 | CONCLUSION AND FUTURE SCOPE

The paper presents the Fuzzy-based Trusted Routing Protocol for vehicular ad hoc networks with unpredictable traffic patterns. In addition to the trusted nodes, the other parameters, such as speed, inter-vehicle distance, connection quality, and the number of nodes in the surrounding area, are considered. The viability of our evaluation method has been shown via several types of testing. In addition, simulations of the new protocol have shown that FTRP can maintain a high packet delivery ratio while adding minimal overhead and lowering end-to-end latency. The simulations of the innovative protocol proved this. We may establish plans for future work to address the impacts of dependability and quality of results of score calculation and include them via scheduling components. These plans may be incorporated into the scheduling components. Future work will likely be carried out that can support infrastructure expansion. In addition to that, addressing the problem of several distinct attack patterns is also possible. We may focus on a decentralized reputation management system to gain granularity in the VCC architecture. Future studies can investigate energy-aware routing algorithms that optimize the selection of relay nodes based on their trustworthiness and energy levels. This would help prolong the battery life of participating electric vehicles and ensure the sustainable operation of VCNs.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Purushottam Sharma https://orcid.org/0000-0002-8037-7152

REFERENCES

Azhdari, M. S., Barati, A., & Barati, H. (2022). A cluster-based routing method with authentication capability in vehicular ad hoc networks (VANETs). *Journal of Parallel and Distributed Computing*, *169*, 1–23.

Bhoi, S. K., & Khilar, P. M. (2016). RVCloud: A routing protocol for vehicular ad hoc network in city environment using cloud computing. *Wireless Networks*, *22*(4), 1329–1341.

Bitam, S., & Mellouk, A. (2015). Cloud computing-based message dissemination pro- tocol for vehicular ad hoc networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9071*, 32–45.

Bitam, S., Mellouk, A., & Zeadally, S. (2015). Bio-inspired routing algorithms survey for vehicular ad hoc networks. *IEEE Communication Surveys and Tutorials*, *17*(2), 843–867.

Chen, J., Mao, G., Li, C., Liang, W., & Zhang, D. G. (2018). Capacity of cooperative vehicular networks with infrastructure support: Multiuser case. *IEEE Transactions on Vehicular Technology*, *67*(2), 1546–1560.

Fadlullah, Z. M., Taleb, T., Vasilakos, A. V., Guizani, M., & Kato, N. (2010). DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. *IEEE/ACM Transactions on Networking*, *18*(4), 1234–1247.

Hafeez, K. A., Zhao, L., Ma, B., & Mark, J. W. (2013). Performance analysis and enhancement of the DSRC for VANET's safety applications. *IEEE Transactions on Vehicular Technology*, *62*(7), 3069–3083.

Igried, B., Alsarhan, A., Al-Khawaldeh, I., Al-Qerem, A., & Aldweesh, A. (2022). A novel fuzzy logic-based scheme for malicious node eviction in a vehicular ad hoc network. *Electronics*, *11*(17), 2741.

Karagiannis, G. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards, and solutions. *IEEE Communication Surveys and Tutorials*, *13*(4), 584–616.

Kaur, R. K. S. (2022). Trust offloading in vehicular cloud networks. In *Recent trends in communication and intelligent systems. Algorithms for Intelligent Systems*. Springer.

Li, F., Wang, Y., & Vehiclesolina, N. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, *2*(2), 12–22.

Li, P., Guo, S., Yu, S., & Vasilakos, A. V. (2012). CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. *Proceedings—IEEE INFOCOM*, 100–108. https://doi.org/10.1109/INFCOM.2012.6195456

Li, P., Guo, S., Yu, S., & Vasilakos, A. V. (2014). Reliable multicast with pipelined network coding using opportunistic feeding and routing. *IEEE Transactions on Parallel and Distributed Systems*, *25*(12), 3264–3273.

Li, W., & Song, H. (2016). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(4), 960–969.

Liang, J., Sheikh, M. S., & Wang, W. (2019). A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs). *Sensors (Switzerland)*, *19*(16), 1–41.

Marwaha, S., Srinivasan, D., Tham, C. K., & Vasilakos, A. (2004). Evolutionary fuzzy multi-objective routing for wireless mobile ad hoc networks. In Proceedings of the 2004 Congress on Evolutionary Computation, *CEC2004*, *2*, 1964–1971. https://doi.org/10.1109/cec.2004.1331137

Meng, T., Wu, F., Yang, Z., Chen, G., & Vasilakos, A. V. (2016). Spatial reusability: Aware routing in multi-hop wireless networks. *IEEE Transactions on Computers*, *65*(1), 244–255.

Nagaraju, R., Venkatesan, C., Kalaivani, J., Manju, G., Goyal, S. B., Verma, C., Safirescu, C. O., & Mihălţan, T. C. (2022). Secure routing-based energy optimization for IoT application with heterogeneous wireless sensor networks. *Energies*, *15*(13), 4777–4789.

Nittu, G., Singh, K., Banda, L., Purushottam, S., Chaman, V., & Goyal, S. B. (2023). ShAD-SEF: An efficient model for shilling attack detection using stacking ensemble framework in recommender systems. *International Journal of Performability Engineering*, *19*(5), 291–302.

Pham, T. D. (2020). *Fuzzy Recurrence Plots and Networks with Applications in Biomedicine*. Springer Cham, eBook ISBN 978-3-030-37530-0. https://doi.org/10.1007/978-3-030-37530-0

Qin, Y., Huang, D., & Zhang, X. (2012). VehiCloud: Cloud computing facilitating routing in vehicular networks. *Proc. of the 11th IEEE Int. Conference on Trust, Security, and Privacy in Computing and Communications, TrustCom-2012—11th IEEE Int. Conference on Ubiquitous Computing and Communications*, pp. 1438–1445.

Onieva, J. A., Rios, R., Roman, R., & Lopez, J. (2019). Edge-Assisted Vehicular Networks Security. *IEEE Internet Things J*. *6*(5), 8038–8045. https://doi.org/10.1109/JIOT.2019.2904323.

Qu, F., Wu, Z., Wang, F., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *16*(6), 2985–2996.

Rostamzadeh, K., Nicanfar, H., Torabi, N., Gopalakrishnan, S., & Leung, V. C. M. (2015). A context-aware trust-based information dissemination framework for vehicu- lar networks. *IEEE Internet of Things Journal*, *2*(2), 121–132.

Shen, J., Wang, C., Castiglione, A., Liu, D., & Esposito, C. (2017). Trustworthiness evaluation-based routing protocol for incompletely predictable vehicular ad hoc networks. *IEEE Transactions on Big Data*, *X*(10), 1.

Shen, Z., Luo, J., Zimmermann, R., & Vasilakos, A. V. (2011). Peer-to-peer media streaming: Insights and new developments. *Proceedings of the IEEE*, *99*, 2089–2109.

Sichitiu, M., & Kihl, M. (2008). Inter-vehicle communication systems: A survey. *IEEE Communications Surveys and Tutorials*, *10*(2), 88–105.

Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., & Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access*, *5*, 15619–15629.

Vasudev, H., & Das, D. (2018). A trust-based secure communication for software-defined VANETs. *International Conference on Information Networking, 2018*, 316–321.

Xiang, L., Luo, J., & Vasilakos, A. (2011). Compressed data aggregation for energy-efficient wireless sensor networks. *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 46–54.

Xi, Xu. R., Ansari, Khokhar, A., & Vasilakos, A. (2015). Hierarchical data aggregation using compressive sensing (HDACS) in WSNs. *ACM Transactions on Sensor Networks*, *11*(3), 45.

Yang, Q., & Wang, H. (2015). Toward trustworthy vehicular social networks. *IEEE Communications Magazine*, *53*(8), 42–47.

Yang, Q., Zhu, B., & Wu, S. (2016). An architecture of cloud-assisted information dissemination in vehicular networks. *IEEE Access*, *4*, 2764–2770.

Yao, J., Feng, S., Zhou, X., & Liu, Y. (2016). Secure routing in multihop wireless ad- hoc networks with decode-and-forward relaying. *IEEE Transactions on Communications*, *64*(2), 753–764.

Yen, Y. S., Chao, H. C., Chang, R. S., & Vasilakos, A. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. *Math. Comput. Model*, *53*(11-12), 2238–2250. https://doi.org/10.1016/j.mcm.2010.10.008

Youssef, M., Ibrahim, M., Abdelatif, M., Chen, L., & Vasilakos, A. V. (2014). Rout- ing metrics of cognitive radio networks: A survey. *IEEE Communications Surveys and Tutorials*, *16*(1), 92–109.

Yu, J., Ren, K., & Wang, C. (2016). Enabling cloud storage auditing with verifiable outsourcing of key updates. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1362–1375.

Yu, J., Ren, K., Wang, C., & Varadharajan, V. (2015). Enabling cloud storage auditing with key-exposure resistance. *IEEE Transactions on Information Forensics and Security*, *10*(6), 1167–1179.

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems*, *50*(4), 217–241.

Zeng, Y., Xiang, K., Li, D., & Vasilakos, A. V. (2013). Directional routing and scheduleing for green vehicular delay tolerant networks. *Wireless Networks*, *19*(2), 161–173.

Zhang, D., Ge, H., Zhang, T., Cui, Y. Y., Liu, X., & Mao, G. (2019). New multi-hop clustering algorithm for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *20*(4), 1517–1530.

Zhang, D., Zhang, T., & Liu, X. (2019). Novel self-adaptive routing service algorithm for application in VANET. *Applied Intelligence*, *49*(5), 1866–1879.

AUTHOR BIOGRAPHIES

Dr. Ramesh Kait is working as Assistant Professor in the Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India. He has presented and published more than seventy papers in International and National Conferences/Journals. His research interests are Wireless networks, VANET and Security in Cloud and Fog Computing, Artificial Intelligence and Machine Learning.

Dr. Sarbjit Kaur received M.Tech degree in Computer Science and PhD degree from Kurukshetra University Kurukshetra in 2010 and 2023 respectively. She is currently an Assistant Professor with Department of Computer Science in Government PG College Ambala Cantt affiliated to Kurukshetra University, Kurukshetra. Her current research interest includes adhoc wireless Network, Cloud Computing, Vehicular Technology and Internet of Things.

Dr. Purushottam Sharma is working as a Professor in the Department of Information Technology, Amity School of Engineering & Technology at Amity University Uttar Pradesh. He has more than 17 years of experience in research, academia, and industry. His research interest includes artificial intelligence, data analytics, temporal data mining, and high-performance networks. Dr. Sharma has published more than 80 research papers in SCI, ESCI, Scopus-indexed journals, and reputed international conferences. He has multiple technical patents in his name. He is a Cisco certified Instructor Trainer ITQ (Instructor Trainer Qualification) and has also obtained CCNA, CCNA (R&S) Global Certificate from Cisco System USA. He has delivered lectures on networking related subjects in e-Learning mode to 29 African Countries using the Pan-African Network at Amity University Uttar Pradesh.

Dr. Chhikara Ankita is currently working as Assistant Professor in PIET, Panipat (affiliated from Kurukshetra University), Kurukshetra. She has received her PhD from Department of Computer Science and Applications, Kurukshetra University in 2023, MCA from Banasthli Vidyapeeth University, Rajasthan in 2016. Her research interests are Artificial Intelligence, Machine Learning, Genetic Algorithm, etc. She had presented various research papers in national/international conferences and also published papers in reputed journals. Moreover, she had filed 3 patents under IPR authority of India.

Tajinder Kumar is an Assistant Professor in the Department of Information Technology Engineering at Seth Jai Parkash Mukand Lal Institute of Engineering and Technology Institute in Radaur. He holds a bachelor's degree in computer science and a master's degree in computer engineering from the Kurukshetra University, Kurukshetra. He is UGC-NET certified in computer science and applications in 2012. His research interests include biometrics, image processing, Software engineering and agile. Mr. Kumar is working in biometric fusion field at the Punjab Institute of Technology. He had published about 08 research papers at international journals and conferences and. Mr. Kumar is a member of international specialist agencies IUCEE, CSI, IAASSE, IAENG, IAOIP and ICAICR.

Dr. Xiaochun Cheng won full scholarship for all his university education, received the BEng Degree in Computer Engineering with first class degree in 1992, PhD in Computer Science with distinction in 1996. Since 1997, has been working in UK University. One project was funded with 16 million Euro budget. He contributed for five times best conference paper awards so far. 6 his papers were in the top 1% of the academic field by Data from Essential Science Indicators. He won 3 times national competitions. He won national award for research. Two solutions achieved national best results and were adopted nationally.

How to cite this article: Kait, R., Kaur, S., Sharma, P., Ankita, C., Kumar, T., & Cheng, X. (2024). Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities. *Expert Systems*, e13561. https://doi.org/10.1111/exsy.13561