Received: 23 May 2022 | Revised: 7 July 2023 | Accepted: 26 August 2023

DOI: 10.4218/etrij.2022-0203

ORIGINAL ARTICLE

ETRI Journal WILEY

Artificial neural network for safety information dissemination in vehicle-to-internet networks

Ramesh B. Koti[1] | **Mahabaleshwar S. Kakkasageri**[2] | **Rajani S. Pujar**[2]

[1]Department of Electronics and Communication Engineering, Gogte Institute of Technology, Belagavi, India

[2]Department of Electronics and Communication Engineering, Basaveshwar Engineering College, Bagalkote, India

Correspondence
Ramesh B. Koti, Department of Electronics and Communication Engineering, Gogte Institute of Technology, Belagavi, Karnataka, India.
Email: rameshkoti1984@gmail.com

Abstract

In vehicular networks, diverse safety information can be shared among vehicles through internet connections. In vehicle-to-internet communications, vehicles on the road are wirelessly connected to different cloud networks, thereby accelerating safety information exchange. Onboard sensors acquire traffic-related information, and reliable intermediate nodes and network services, such as navigational facilities, allow to transmit safety information to distant target vehicles and stations. Using vehicle-to-network communications, we minimize delays and achieve high accuracy through consistent connectivity links. Our proposed approach uses intermediate nodes with two-hop separation to forward information. Target vehicle detection and routing of safety information are performed using machine learning algorithms. Compared with existing vehicle-to-internet solutions, our approach provides substantial improvements by reducing latency, packet drop, and overhead.

KEYWORDS

Bayes' rule, dynamic clustering, Levenberg–Marquardt algorithm, safety information, software agent, vehicular ad hoc network

1 | INTRODUCTION

In transportation, vehicular ad hoc networks (VANETs) offer various services to improve comfort and safety. Hence, the automotive industry has expanded rapidly and now offers such services. Vehicles (nodes) are wirelessly connected to roadside equipment, cloud centers, digital video broadcasting units, and other vehicles in vehicle-to-internet (V2I) communications. A variety of resources on the roadside can improve connectivity between vehicles. Medium access protocols with short channel vulnerability times are used to primarily reduce packet collisions [1]. VANETs have received considerable attention in intelligent transportation owing to the development of the Internet of Things and fifth-generation (5G) communications. As a result, safety information can be delivered to vehicles farther and more quickly than ever before [2]. Cloud services assist source vehicles in quickly locating destination vehicles. Nevertheless, the low processing power of mobile nodes renders the identification of reliable targets challenging. Thus, cloud servers, roadside units (RSUs), and smartphones can participate in V2I communications to guarantee the distribution of information with negligible network overhead [3].

Various issues related to vehicle-to-vehicle and V2I communications have been resolved using V2I communication methods. Cloud-based services with GPS (global positioning system) navigational capabilities have been used to discover credible targets. During travel, an RSU performs an intensive search for neighboring clouds. To reduce overhead, two-hop message transmission is implemented. By excluding non-safety events, node search in the source vehicles can further reduce overhead. In [4], energy-efficient cluster intradomain routing is achieved. Based on target prediction, nonparticipating vehicles turn into sleeping nodes to save energy.

An RSU has wired connectivity, mitigating network link failures and establishing several node data routes. Therefore, the data processing load on the end nodes is reduced. The cloud is an infrastructure in which machine learning techniques can be deployed for reliable navigation to perform target node discovery [5]. An information dissemination scheme using a software agent approach is introduced in [6]. The agents use real-time data and perform specific tasks. Data integrity is protected and maintained through V2I communications. Hence, the packet delivery ratio is improved while reducing overhead.

In this study, we developed an artificial neural network (ANN) based on Bayes' rule (BR) optimization and the Levenberg–Marquardt algorithm (LMA) to classify safety events and process data while preserving stable communication. The increasing use of smart technologies has drastically enhanced the reliability of connectivity, secure wireless transmission, and efficient processing. However, various computational and communication challenges persist regarding data augmentation in networks. The gradient-based local optimization of the LMA is deterministic and offers a rapid average convergence and system stability, which can benefit multistage perceptron training.

1.1 | Motivation

Numerous methods for vehicular networks have improved information sharing. However, in the future of vehicle transportation, various activities will be possible, such as holding conference meetings while driving, driving without stress, or even sleeping. Thus, integrating services from various communication technologies is required for VANETs. Automated processes and various applications exist for selecting these services. Suitable routing and path prediction are required to locate a target node when processing massive vehicular data. Thus, the end-to-end latency should be reduced while improving the packet delivery ratio. Existing developments have inspired us to develop an enhanced V2I communication environment.

Our V2I network is intended to provide vehicles with an effective and stable connection that enables a dependable and secure transportation system. It may help to prevent accidents, perform immediate rescue operations, improve vehicle and driver safety, and make transportation systems more secure and comfortable. Depending on the system requirements, all the information from vehicle sensors can be intelligently routed through a gateway node and communicated to an RSU or broadcasted to surrounding vehicular clouds. In addition to dissemination of road safety information, various levels of data processing are incorporated at different levels of the network nodes to prevent overload.

1.2 | Contributions

We combine machine learning methods, cloud computing power, and wireless technology to improve the performance of V2I communications. The main contributions of our study are summarized as follows: (1) grouping vehicles according to their distances to form vehicle clusters, (2) relaying sensor-activated safety and non-safety event information using two-hop communication, and (3) discovering target nodes using machine learning techniques running in the cloud and RSU. The tasks for V2I information dissemination are described as follows:

- Vehicles are clustered based on the communication range along the road. The vehicles monitor and detect key events on the road, such as accidents, traffic density, land sliding, and excessive fog, using onboard sensors.
- Dynamic clusters are created by grouping the nodes on the road according to their communication range. The cluster head (CH) is selected based on the distance from the RSU and by using processing resources among the available nodes to route traffic from the end nodes to the RSU.
- Within a cluster, information forwarding is always performed using the two-hop link lifetime-based algorithm (THLLBA) with two-hop data forwarding by selecting the links with the longest connection time. These links provide reliable connectivity to improve the throughput and reduce latency.
- Information is forwarded from the RSU to a nearby vehicular cloud and then to the internet through wired connections to enable efficient channel access for reliable target detection.

When safety information enters the cloud center, the message type is identified. For example, if the safety message refers to an accident, the target node may be a hospital or a nearby rescue station. To discover reliable targets, machine learning techniques are used, such as the LMA.

The remainder of this paper is organized as follows. Section 2 describes related work on techniques, difficulties, shortcomings, and future developments related to V2I safety information transmission. In Section 3, we detail the static and mobile agents used in our approach and existing solutions. Section 4 describes the simulation analysis along with the inputs and parameters. Section 5 highlights the simulation results. Finally, we draw conclusions in Section 6.

2 | RELATED WORK

Vehicle-to-network or V2I communication comprises both vehicle-to-vehicle and V2I networks as well as internet services. A supporting architecture is required to extend and enhance the range of communication and increase the number of internet services. Requested information can be sent to vehicles that are not currently within the roadside infrastructure range through multiple hops [7]. Vehicle-to-network communication allows to connect the target and source nodes using an optimal path that improves the packet delivery ratio. This is achieved through roadside infrastructure and internet cloud units, which act as intermediate nodes.

Major enabling technologies in vehicle-to-network communications involve various areas such as novel materials, algorithms, and system designs, as discussed in [8]. Machine learning has gained popularity in intelligent transportation systems for vehicle-to-network communications that deliver services under stringent requirements. However, dedicated short-range communication has substantial limitations, such as limited coverage, low throughput, poor quality of service, and long channel access latency, in crowded and high-mobility environments [9]. A comprehensive overview of the vehicle-to-everything ecosystem is presented in [10]. In this ecosystem, primary security/privacy concerns, current standardization efforts, and potential defensive measures are being addressed [11]. In addition, the taxonomy of misbehavior detection mechanisms and state-of-the-art vehicle-to-everything security solutions have been analyzed.

A social vehicle-to-everything communication model has been proposed to improve the flow of traffic in intelligent transportation systems by transmitting required information in time using ultrahigh-speed integrated cellular 5G technology [12]. This model notably improves information transmission for moving vehicles. Because wireless communication is broadcasted, it is vulnerable to jamming, eavesdropping, and spoofing, which may harm an intelligent transportation system. Hence, intelligent vehicle-to-everything security is devised in [13]. Multiagent driven clustering for VANETs is presented in [14]. A route is predicted using the vehicle speed, travelling direction, degree of linkage to other vehicles, and mobility pattern.

In [15], both weighted and non-weighted static agents are incorporated. First, during dynamic clustering, the cluster members are chosen according to the relative speed and direction of the vehicles. CHs are selected from the members based on a stability measure derived from the degree of connection, average speed, and time required to depart the road junction. Dual-channel transmission involving control and service channels is used by the protocol to ensure service performance that is sensitive to certain delays [16]. A quick overview of current technologies, standardization, and existing technology capabilities is presented in [17].

In [18], various problems, trends, and possible solutions for V2I communication are addressed. Network resources are assigned to vehicular nodes by considering an inexpensive model. However, the overall system implementation to improve efficiency is complex. The existence of additional infrastructure enables vehicle-to-everything services to substantially improve the throughput, bandwidth utilization, and packet overhead. In [19], various scenarios are examined for recent and sophisticated autonomous driving applications. In addition, the management by fourth-generation and 5G networks of the latency and spectrum requirements of various use cases is analyzed.

To prevent attacks during communication, appropriate security and authentication mechanisms are required [20]. However, authentication may compromise user privacy by carrying location and identity information. User privacy can be protected using cryptography, but it is intended to be deployed in a third-party server. Consequently, conventional security models suffer from communication and key management overhead. To address this problem, a secure performance-enhanced channel-allocation security model based on the commutative RSA (Rivest–Shamir–Adleman) system is proposed in [21]. In [22], cell-based data transactions in intelligent transportation systems are analyzed emphasizing path setup delay and time overhead. The uniqueness of transportation networks demands the deployment of specific security methods to address problems with vehicle-to-everything communication. For instance, blockchains may ensure the secure exchange of information [23].

In [24], multipath routing minimizes the path recognition time, end-to-end delays, and routing overhead to decrease the complexity and increase the quality of service. A reduced broadcast overhead for an emergency message scheme is proposed in [25]. To overcome the broadcast storm problem, dynamic clustering is used by incorporating a novel CH selection mechanism. The vehicles with the most stable connectivity are selected as CHs, thereby assisting in the transmission of emergency information with reduced packet collisions.

In vehicular cloud networks, efficient resource management increases resource utilization and reduces costs. Similarly, appropriate resource allocation reduces costs, vehicle (client) waiting times, and waiting queue lengths. A cost model can allocate resources to vehicles using the least costly route, thereby resulting in cost savings. In [26], a dynamic resource discovery technique for a vehicular cloud network is introduced. A resource-finding strategy using honeybee optimization is combined with static and mobile agents in [27]. The mobile agents collect vehicle cloud information, and the static agents identify the resources required by the vehicles.

A vehicular cloud is a resource pool that stores, processes, navigates, and provides network services to all vehicles within the communication range. It enables the timely delivery of data to achieve road safety, efficient information exchange, and fast transmission of safety warnings [28]. The Internet of Everything may eventually integrate mobile devices, desktop computers, and laptops for real-time data exchange [29]. In a V2I communication system, vehicles can communicate easily with each other on the road with support of the infrastructure they pass through while traveling, cloud-based software, and a covered power grid [30]. In [31], a Bayesian game model is proposed to find the optimal node for data transmission in a wireless sensor network by considering energy, bandwidth, and computational latency.

Various dissemination techniques have been analyzed and evaluated in V2I networks, identifying the following limitations: lack of intelligence in dissemination, inadequate handling of vehicle dynamics, link duration inconsistency, and scalability issues. Our proposed approach addresses these limitations, and we perform a comparison with existing studies to evaluate the performance improvements.

3 | PROPOSED APPROACH

We propose a multiple cluster architecture with ANN-based safety information dissemination for V2I communication in VANETs. The proposed approach collects safety information from onboard vehicle sensors, and the THLLBA allows to disseminate this information. Forwarding nodes at two hops with reliable connections are selected based on the duration of their connections. Smart algorithms based on artificial intelligence (AI) are used to analyze data and disseminate safety information throughout the network with a short end-to-end delay. The proposed approach is intended to efficiently transmit information from a source vehicle with enhanced end-to-end latency, travel time, flow velocity, and communication overhead.

3.1 | Network scenario

The scenario for the proposed approach to establish V2I communication is shown in Figure 1. The clusters are enclosed in dotted circles and comprise high-density moving nodes (N1–N9) traveling at different speeds and gateway nodes GN1–GN4 that perform packet routing between the end nodes and RSUs. Information forwarding within the cluster is performed through dedicated short-range vehicle-to-vehicle communication (dotted arrows in Figure 1). A high-speed cable network connects RSUs RSU1–RSU4 to vehicle clouds for information transmission (solid arrows). Vehicular clouds VC1 and VC2 collect information of distant nodes within the communication range. The information includes relative speed, location coordinates, vehicle identifier, and driver information. The network consists of several clouds. A vehicular cloud can access internet services to incorporate additional features, and internet access is achieved by an infrastructure-based interface. The vehicle GPS coordinates and information about road junctions are sent to the cloud using an internet service, facilitating the selection of reliable targets by the cloud.

3.2 | Node clustering

Information dissemination begins with clustering, which includes the identification of reliable nodes to form a cluster and CH selection. The CH announces vehicle mobility patterns, and cluster formation is based on the relative speed difference in a small area. All the nodes are instructed by the CH to broadcast their speeds according to their communication ranges. Vehicles are considered neighbors if the distance between them is less than R. Neighboring vehicles traveling in the same direction and lane are evaluated for clustering, whereas those traveling in the opposite direction are discarded. Vehicles are clustered according to the communication range along the route. The CH is selected according to its distance from the RSU and capacity to handle traffic routing between the end nodes and RSU.

3.3 | Safety message classification

Onboard sensors in each vehicle allow to identify events based on measurements, and rainforest search is applied to determine the type of event. This technique categorizes massive data based on attribute values and class labels through supervised learning on multiple events and by combining several classifiers to improve performance. The classification accuracy depends on the responses of

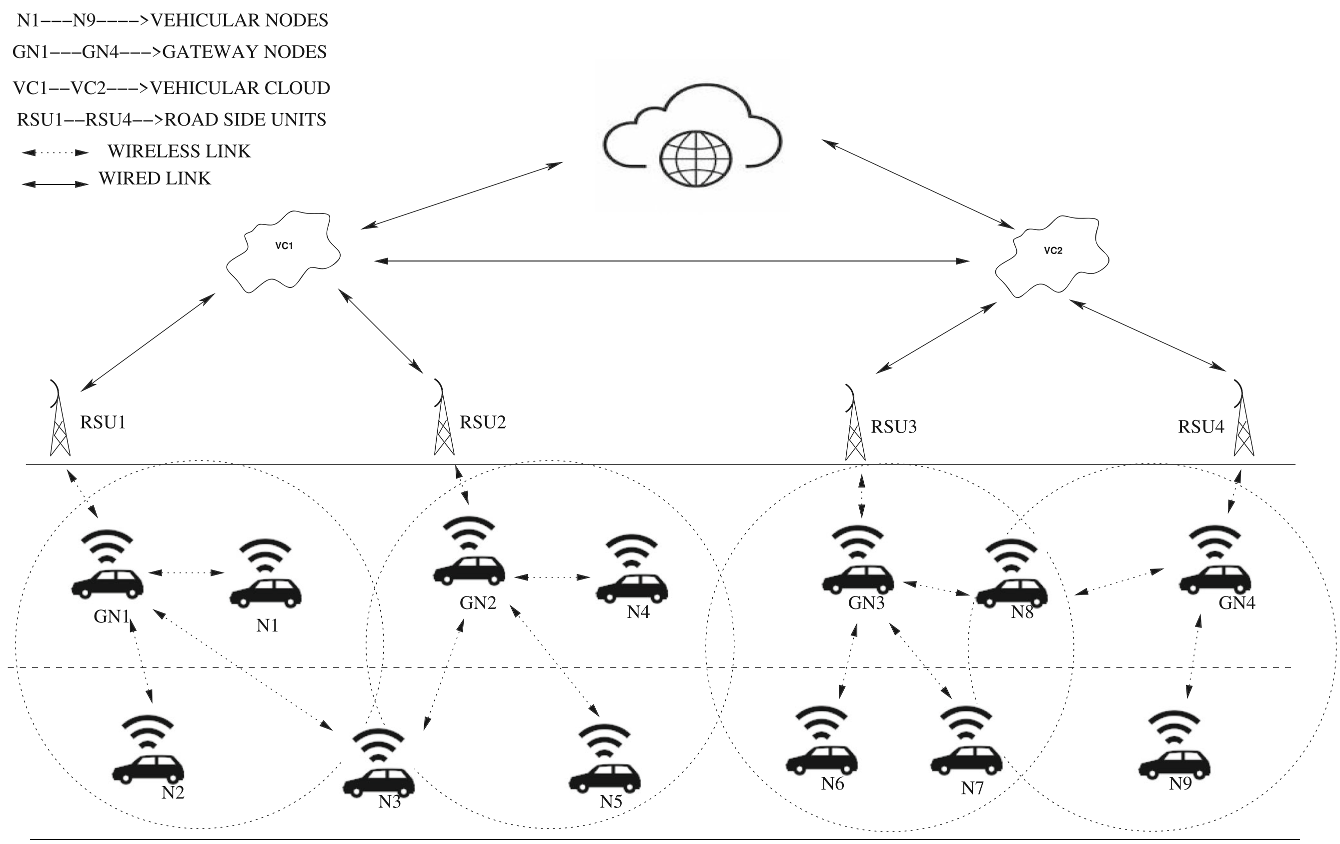

FIGURE 1 Architecture of proposed V2I network.

multiple decision trees and subsets of training samples. From various measurements, events are categorized as either safe or dangerous. The safety and non-safety events according to the sensor states and corresponding target stations are listed in Table 1. The target nodes are identified based on the type of safety information to avoid broadcasting safety data to all the nodes in an area. Thus, secure and fast delivery of data is achieved with energy efficiency.

3.4 | Functional model using agents

In AI, a software agent makes intelligent decisions based on predictions and can accurately perform a specific task. Software agents can perceive the environment through sensor measurements to perform corresponding actions using actuators. In the proposed approach, information fetching from moving vehicles is assigned to software agents called mobile agents. Different types of agents collaborate for data dissemination, as detailed below.

- **Vehicle agency**: The vehicle agency for the proposed approach is illustrated in Figure 2. This agency is implemented in the base layer of the network and comprises two agents. The mobile agent (information collection agent) collects traffic information from neighboring vehicles in the communication range, and the vehicle manager agent coordinates the activities in the communication system. The information is updated in a knowledge base at regular intervals or by a trigger state.
- **RSU agency**: The second-level RSU agency finds vehicular clouds in its communication range for information forwarding. The messages are destined to the RSU from the bottom layer using two-hop switching to accelerate transmission. The bottom layer also discards non-safety messages from dissemination to avoid information flooding. Hence, unnecessary delayed data determined from a counter (timer) are discarded from the network to further reduce flooding. During the scheduled time to live, data are sent across a wired fiber connection to a vehicular cloud. The vehicle manager agent oversees the RSU operations.
- **Vehicular cloud agency**: The network cloud holds the information about safety and non-safety events in a matrix that can describe any event listed in Table 1. To identify a reliable target vehicle, the vehicular cloud

TABLE 1 Safety and non-safety events according to sensor measurements.

Crash sensor	Wiper state	Engine state	Vehicle speed (m/s)	Emergency alert	Safety event	Target station
ON	OFF	OFF	0	OFF	Accident	Hospital
ON	ON	ON	0	ON	Accident	Hospital
OFF	ON	OFF	10	OFF	Land sliding	Fire station
OFF	OFF	ON	20	OFF	High traffic density	Traffic station
OFF	OFF	OFF	0	ON	Empty fuel	Fuel station
OFF	ON	ON	30	ON	Heavy rain/fog	Weather station
ON	ON	ON	0	ON	Accident	Hospital
ON	ON	ON	0	ON	Accident	Hospital
OFF	ON	OFF	30	ON	Heavy rain/fog	Weather station
OFF	OFF	OFF	20	ON	Critical event	Broadcast
ON	OFF	OFF	0	OFF	Accident	Hospital
OFF	OFF	OFF	30	OFF	High traffic density	Traffic station
ON	OFF	OFF	0	ON	Accident	Hospital
OFF	OFF	OFF	20	OFF	Land sliding	Fire station
OFF	OFF	OFF	0	ON	Empty fuel	Fuel station
OFF	OFF	OFF	30	ON	Critical event	Broadcast

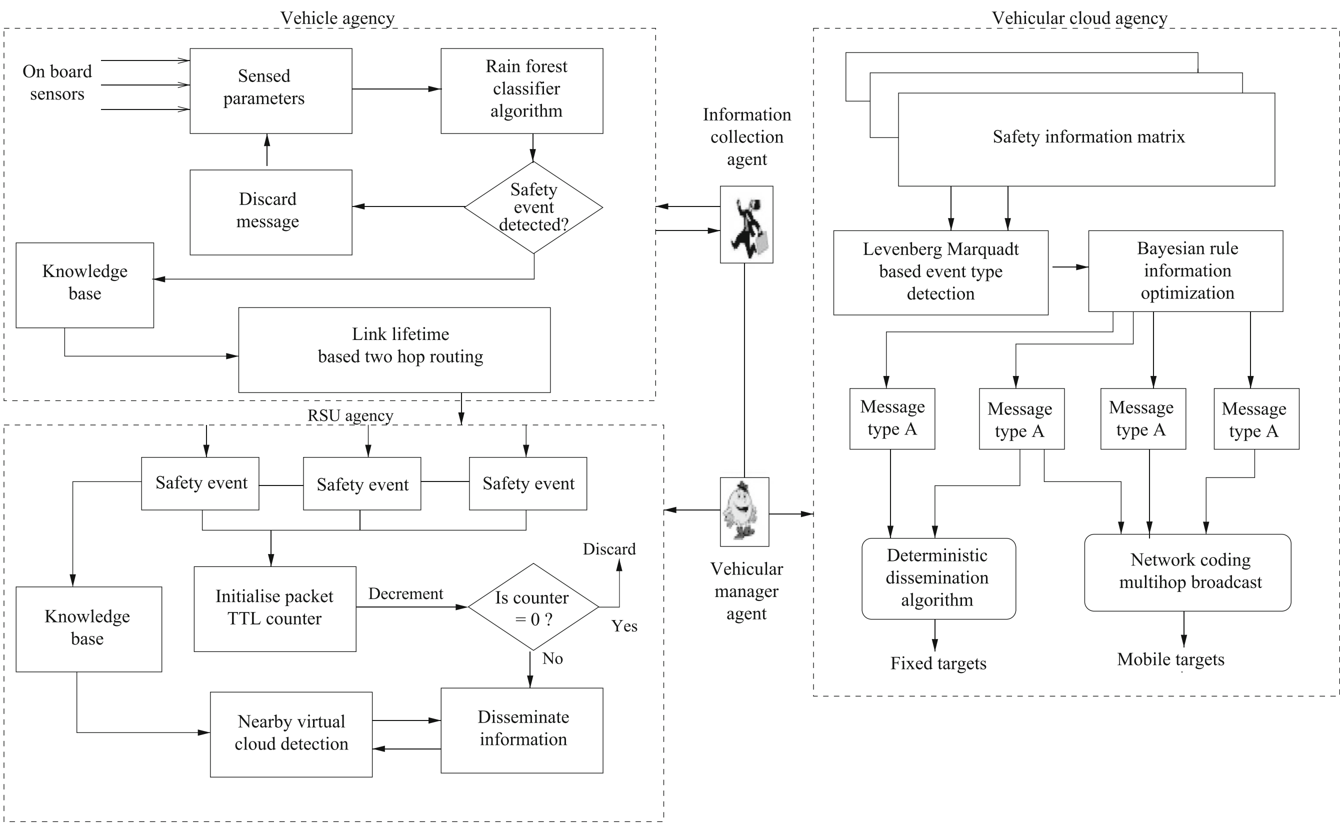

FIGURE 2 Vehicle agency function model.

implements the LMA and BR optimization to correlate targets based on the type of safety information. The functions of the vehicular cloud agency are indicated in Figure 2. The messages are either critical or non-critical, and they are identified by the BR optimizer. Fixed targets include fuel and weather stations as well as hospitals, and they serve as destinations for vehicles. For efficient dissemination to different targets, deterministic and network coding broadcast methods are used. This approach enables the vehicular cloud to select an adequate target quickly and efficiently. For instance, if an accident occurs, the information is sent to a nearby hospital and police station, initiating rescue efforts and preventing unnecessary broadcasting to irrelevant target stations. The sensor measurements allow to identify safety events. For example, after an accident occurs, the crash sensor is activated, the engine turns off, and the vehicle speed is 0. An emergency alert is controlled by the driver to trigger an emergency state. Table 1 details the possible events based on sensor measurements.

3.5 | Target node discovery and dissemination

Table 1 is constructed according to various suggestions and by removing redundancies. The vehicle speed is represented by a continuous value. Several machine learning, trust-based, and AI algorithms have been proposed for node detection. Smart and AI-based Internet-of-Things schemes are suitable for various applications and maintaining safe communication among network nodes. We propose an AI-based hybrid vehicular network to process and compute massive data in a distributed method that ensures fast secure communication. The target nodes are identified based on the type of safety information to avoid broadcasting to all the nodes in an area.

An AI-based ANN is a mathematical model for implementing data categorization, nonlinear functions, and regression. The proposed AI-based ANN architecture comprises inputs from multiple embedded sensors, data manipulation units, backend layers, and an output unit, which identifies the target vehicle. The AI-based ANN has o outputs, H_h backend units, and I_i inputs, and it is described by

$$\alpha_r(t) = \sum_{\alpha=1}^{H_k} W_{rs}^2 F(.) \sum_{y_1} I_i W_{ar}^1 \alpha_s(t)^0 + b_{ar}^1, \text{ where } 1 \le r \le 0, \tag{1}$$

with W_{rs} and W_{ar} representing the edge connectivity values between the input, middle, and output layers. In addition, F is the sigmoid activation function that determines a suitable target regarding processing and computation using the ANN. Weights W_{rs} and W_{ar} determine an appropriate scheme for optimization based on the LMA and BR optimization. Incorporating an AI-based scheme into an Internet-of-Things system to process or safeguard multihoming network data can be beneficial. In the following subsections, we explain the LMA and BR optimization used to obtain accurate outputs.

3.6 | LMA

The LMA is a deterministic gradient-based local optimization method. While training a multistage perceptron, the LMA provides a quick and consistent convergence rate while ensuring system stability. The LMA defines a trust region for finding the minimum of a function. In the proposed approach, various types of data (safety/non-safety) must be delivered to specific targets by identifying them with a short end-to-end delay. Even for various dependent and independent variables, the LMA allows to quickly find a reliable target.

The LMA was created for a second-order derivation training speech technique without estimating the Hessian matrix, which is analogous to a quasi-Newton system. By applying the sum of squares, the Hessian matrix ($\mathbf{H}_M$) is approximated as follows:

$$\mathbf{H}_M = \mathbf{Q}^{\mathrm{T}}\mathbf{Q}, \tag{2}$$

$$\mathbf{G} = \mathbf{Q}^{\mathrm{T}}\sigma, \tag{3}$$

where $\mathbf{Q}$ is a Jacobian matrix that holds the sensor measurements according to biases and weights, thus representing an error vector in an ANN. This Jacobian matrix can be assessed by applying BR optimization, with the predictions from the hidden layers being represented as

$$\alpha_q(t) = F'(I_i(t)) \sum_q \sigma_q^r(t) W_{rq}^2(t-1), \tag{4}$$

where q is the number of safety event neurons over r hidden layer neurons (safety/non-safety events). Furthermore, the LMA uses the following Hessian matrix approximation:

$$\text{delta(w)} = -\left[\mathbf{Q}^{\mathrm{T}}\mathbf{Q} + \mu I\right]^{-1} \mathbf{Q}^{\mathrm{T}}\sigma, \tag{5}$$

where w indicates the governing parameters and indicates differential weights. If μ is zero, the Newton method is obtained. Otherwise, for large μ, a gradient descent with short steps is obtained. Near the minimum error, the Newton method is substantially more accurate and faster. Hence, we decrease μ after each successful procedure and increase it only when the step improves the performance function.

3.7 | BR optimization

To improve the processed data, we combine the LMA with BR optimization to determine the targets for information dissemination. BR optimization is described as

$$P(x|I) = \frac{P(I|x)}{P(I)}. \tag{6}$$

The prior probability of x before obtaining the processed information is represented by $P(x/I)$, whereas $P(x/I)$ is the likelihood of locating the probability of information I. The posterior probability of x given I is represented by a BR. The distribution across all possible values of x is also provided by the BR. This process is used to generate the probability distribution across weights w for an ANN when the training data are represented as $P(w|I)$.

$$P(w|I) = \frac{P(I|w)P(w)}{P(I)}, \tag{7}$$

$$P(w|I) = \frac{P(I|w)}{\delta P(I|w)P(w)dw}. \tag{8}$$

In the formulation of the BR, the learning of weights alters beliefs about the past, $P(w)$, and posterior, $P(w/I)$, weights. When data are gathered and processed from multiple input changes, the learning rates also change. Moreover, the inputs from malicious nodes can be analyzed using the network energy usage and distribution ratio. In fact, malicious nodes always process false or contradictory information, generating many mistakes.

The inputs are subjected to the LMA to determine the convergence rate and weights (trust) of each node input while recording errors. The gradient and Jacobian matrix are evaluated for every node, including the hidden nodes. The regulating parameters represented in (4) and (5) are used to handle mistakes when analyzing the weights from various input nodes.

The Newton method is also used to obtain rapid and accurate results while minimizing errors. The BR is applied over the LMA to optimize the processed or recorded information from the inputs for efficient processing and weighting. This is performed after assessing or calculating the weight of each node. The input is distributed based on probabilities to the different nodes to compute (refer to (6)) and process the efficient distribution of information while maintaining system stability. Both (7) and (8) describe the optimal stationary and mobile targets used to forecast the dissemination strategy.

3.8 | Operational sequence

The operational sequence of the proposed approach is as follows. (1) Based on the communication range along the route, vehicle clustering is performed. (2) The CH is selected based on the distance from the RSU and the node capacity to handle traffic routing between end nodes and the RSU. (3) A two-hop node link lifetime approach is used to relay the information inside a cluster, where switching occurs between a few nodes in the cluster to avoid redundancy. (4) Connections with the longest connection times are chosen for information dissemination.

Data are sent from the RSU to a nearby vehicular cloud and internet devices through a wired connection, which ensures accurate target recognition. Two ANN approaches based on the LMA and BR optimization improve the accuracy of dissemination. The operational sequence is performed in synchronization with the vehicle, RSU agency, and cloud agency modules. We evaluated the latency of the proposed approach based on the cumulative delay associated with the three modules.

3.9 | Algorithms

Algorithm 1 details the proposed procedure for cluster formation. The inputs are all the vehicle distances and movement directions. Initially, CH advertisement CHA is hosted by a node at random, and all other nodes in the communication range receive the CHA packet.

The cluster members respond by cluster membership request CMR from the CH, which determines the distance and direction during selection of cluster members and acknowledges the node for registration using a confirm packet.

Algorithm 1 Cluster formation and CH selection

```
Input
dst: distance of vehicle i
dir: direction of vehicle i
Output
Formed cluster
if CHA ← Recv() then; IN receives CHA from CH
    Send(CMR)    ; Send CMR to CH
end if
if CMR ← Recv() then
    if dst_CH = dst_IN and dir_CH = dirin then
    Send (M_confirm )
    else
    Discard 0
    end if
end
```

Algorithm 2 Emergency message dissemination

```
Input
M_i: input message
T_x: destination node
Information transmitted
1: M_i → Recv0
2: if M_i is critical data, then
3: if T_x activates BR optimization, then
4: T_d = T_d − 1
5: if T_d ≠ 0
6:     Send (M_i)
7:     Perform transmission
8:     else if Suspend transmission
9:     wait for new input and go back to line 1
10:    end if
11: end
```

Algorithm 2 shows the procedure for disseminating an emergency message. The RSU receives sensor data from the end nodes and identifies critical or non-critical information accordingly. If the message type is emergency, information broadcasting is performed based on the target node identified using BR optimization. Otherwise, broadcasting is suspended, and the emergency message is only transmitted to certain target stations to reduce dissemination overhead and accelerate transmission.

The LMA delivers a rapid and constant convergence rate that ensures system stability, being suitable for training multistage perceptron models. BR optimization assists in the selection of reliable targets for dissemination until T_d reaches zero.

4 | SIMULATION

The proposed agent-based aggregation model was simulated in Python as a discrete event system. The inputs for the simulation and performance measures are detailed in this section. The simulation was performed at various time intervals to cover overall topological changes. After the initial 180 s of registration, the agents collected the data. To obtain stable outcomes, the simulation was run five times. The network, traffic, mobility, and channel models as well as the optimization algorithms are described in this section. A network range length of 20 km was considered with RSU interleaving of 5 km and placement of a vehicular cloud at 5 km per RSU. The packet header included additional data to reflect the number of targets, channel contention, and route congestion.

- **Packet delivery ratio**: This ratio (in percentages) is defined as the ratio of the total number of packets sent by the source to the total number of packets received at the destination during any communication between the two parties. This ratio reflects the network performance.
- **Link lifetime**: The link lifetime (in seconds) is defined with respect to consistency or availability of an active link for information exchange. In wireless communication, stable connection is difficult to sustain over a long time. Hence, this measure reflects the connection stability in a network.
- **End-to-end delay**: The time elapsed to deliver a complete message to a distant target vehicle is known as the transmission delay (in milliseconds). It depends on the vehicle density, dynamic topology, and number of intermediate nodes.
- **Dissemination efficiency**: It measures the efficiency of transmission considering the end-to-end delay and latency. It is expressed as

$$DE = \frac{\text{Propagation distance} \times \text{Success ratio}}{\text{Propagation time} \times \text{Redundancy rate}}. \tag{9}$$

- **Cluster stability**: It is defined as the duration (in seconds) of the connection between the CH and cluster members. It indicates the connectivity consistency.
- **RSU response time**: It is the time difference (in seconds) between packet arrival (uplink) and packet dispatch (downlink) at an RSU. This measure is the crucial part of the response time that affects the end-to-end delay.

- **Routing overhead**: The overhead is the additional time (in milliseconds) required for packet transfer. It includes the delays of handshaking, node registration, and storing and forwarding.
- **Network redundancy rate:** This rate (in percentages) is defined as the availability of multiple pathways between source and destination vehicles. Multiple links provide flexibility for maintaining the connection under node route failures.

The abovementioned performance measures were obtained to confirm the considerable improvements of our approach through simulations. These improvements were due to the additional cloud network facility and THLLBA, which were simulated in Python.

5 | RESULTS AND DISCUSSION

To evaluate the performance of the proposed approach, we obtained various performance measures (Section 4) according to the vehicle (node) density and mobility level. To verify the effectiveness of the proposed approach, we compared its results with those of the position-based emergency message dissemination for internet-of-vehicles (PEMIV) scheme.

At various vehicle densities, the packet delivery ratio, energy consumption, routing overhead, cluster formation time, and average end-to-end latency of the dissemination strategies were examined (from 10 to 100 vehicles).

- The packet delivery ratio according to the vehicle density is shown in Figure 3 for different mobility levels. The high-quality links and two-hop forwarding of the proposed approach lead to higher performance compared with the PEMIV scheme. However, at low vehicle density and increased mobility level, the performance of the proposed approach drops by 8%.
- The link lifetime indicates the availability of a communication channel for transmission, as shown in Figure 4. The long connectivity duration and two-hop forwarding of the THLLBA improves the link lifetime by 20% when compared with the PEMIV scheme.
- Figure 5 shows the effects of vehicle density on the end-to-end latency. With more mobility and lower vehicle density, the average latency increases. More vehicles facilitate finding dependable nodes along the route, and the cellular infrastructure network in the RSUs and cloud can swiftly analyze safety data using the LMA and BR optimization. The total delay

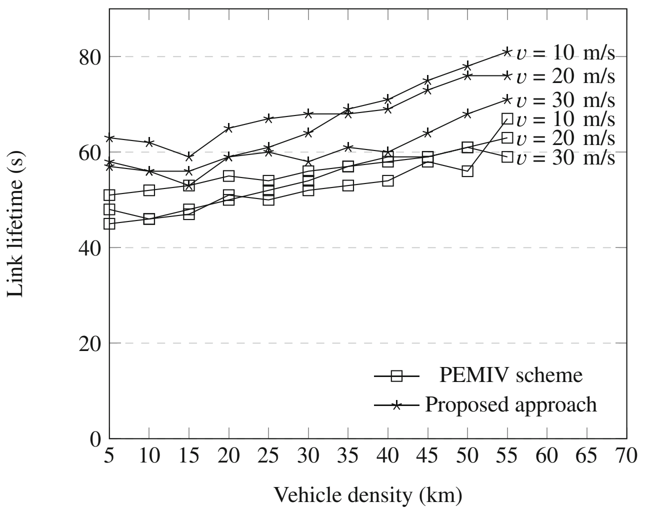

FIGURE 4 Link lifetime according to vehicle density.

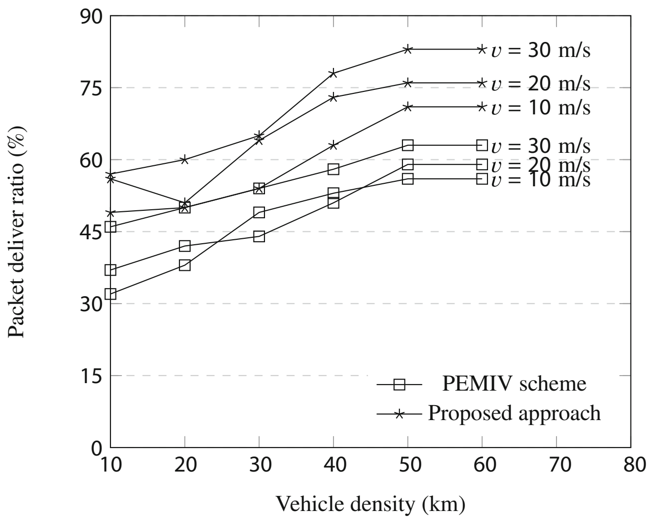

FIGURE 3 Packet delivery ratio according to vehicle density.

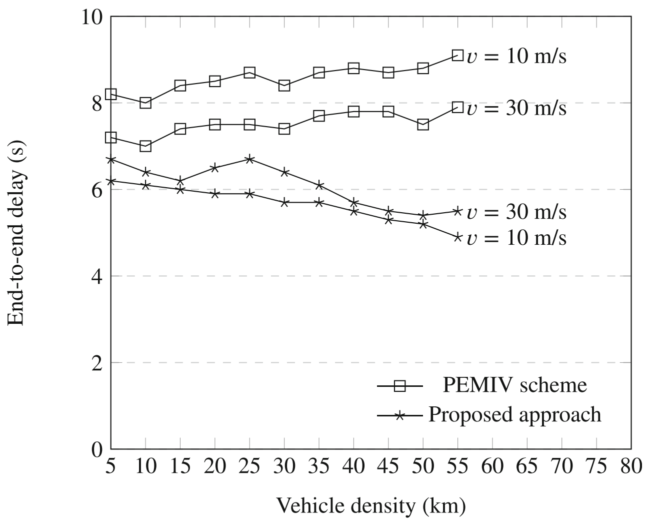

FIGURE 5 End-to-end delay according to vehicle density.

includes forwarding and processing times. At greater mobility levels, the proposed approach consistently has the longest latency, possibly because route finding takes a long time owing to inconsistent network connections. At increasing vehicle density, the proposed approach offers a shorter end-to-end delay than the PEMIV scheme.

- Figure 6 shows the dissemination efficiency according to the vehicle density. Given the steady connectivity for a long period and possible prevention of collisions, a gain in efficiency is achieved for longer link lifetimes. Additionally, two-hop forwarding decreases the quantity of intermediate vehicle nodes, mitigating the processing of redundant data. The efficiency increases by all these factors.
- Cluster stability indicates how often the cluster configuration changes when the scenario changes. The duration of a CH using the proposed approach according to the vehicle density and mobility level is shown in Figure 7. As the vehicle mobility increases, the CH stability decreases because the network topology changes more rapidly. Hence, the CHs are unable to remain stable with the same cluster members over long periods. The THLLBA uses two-hop clustering, in which the CH may reach all nodes two hops away, and the CH is chosen according to the lowest velocity.

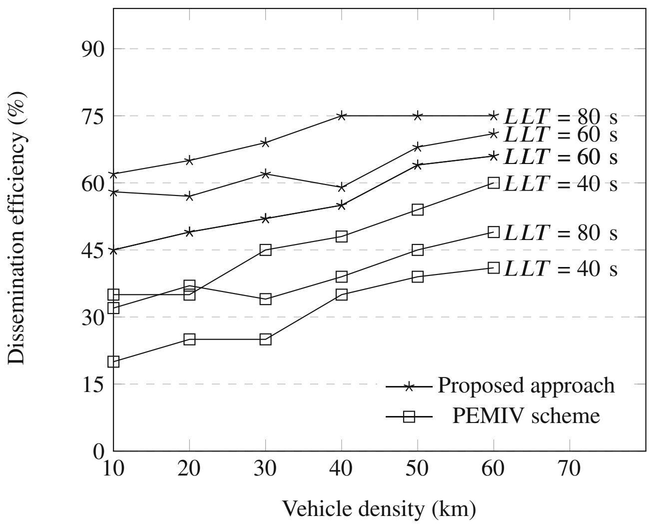

FIGURE 6 Dissemination efficiency according to vehicle density.

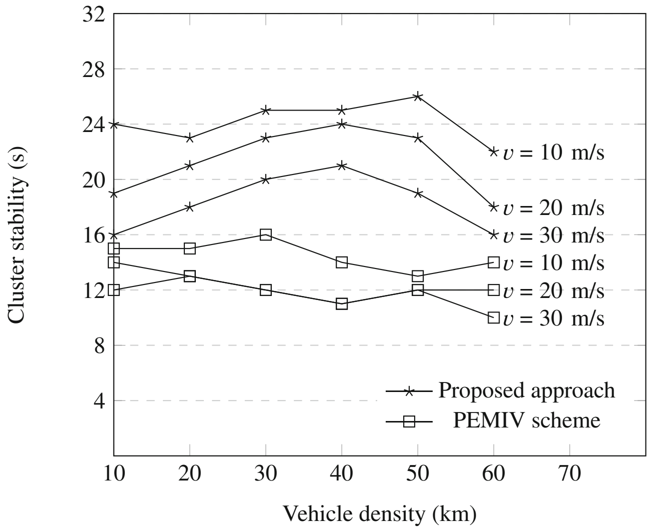

FIGURE 7 Cluster stability according to vehicle density.

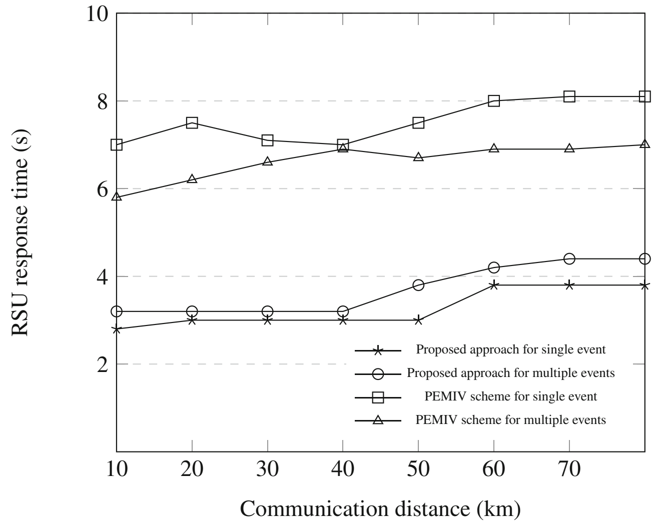

FIGURE 8 RSU response time according to communication distance.

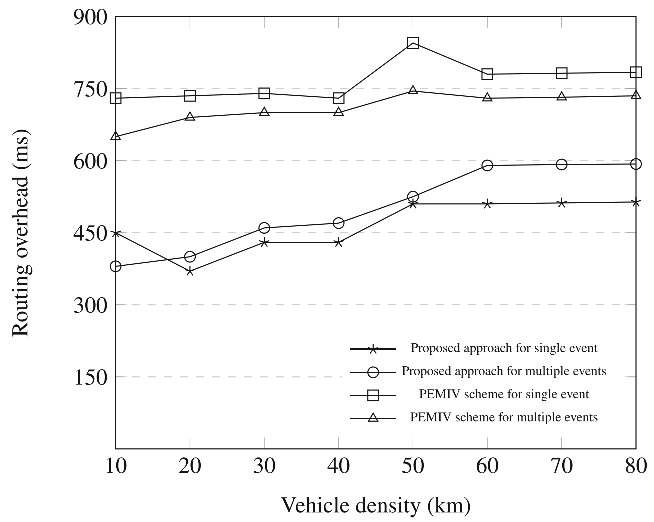

FIGURE 9 Routing overhead according to vehicle density.

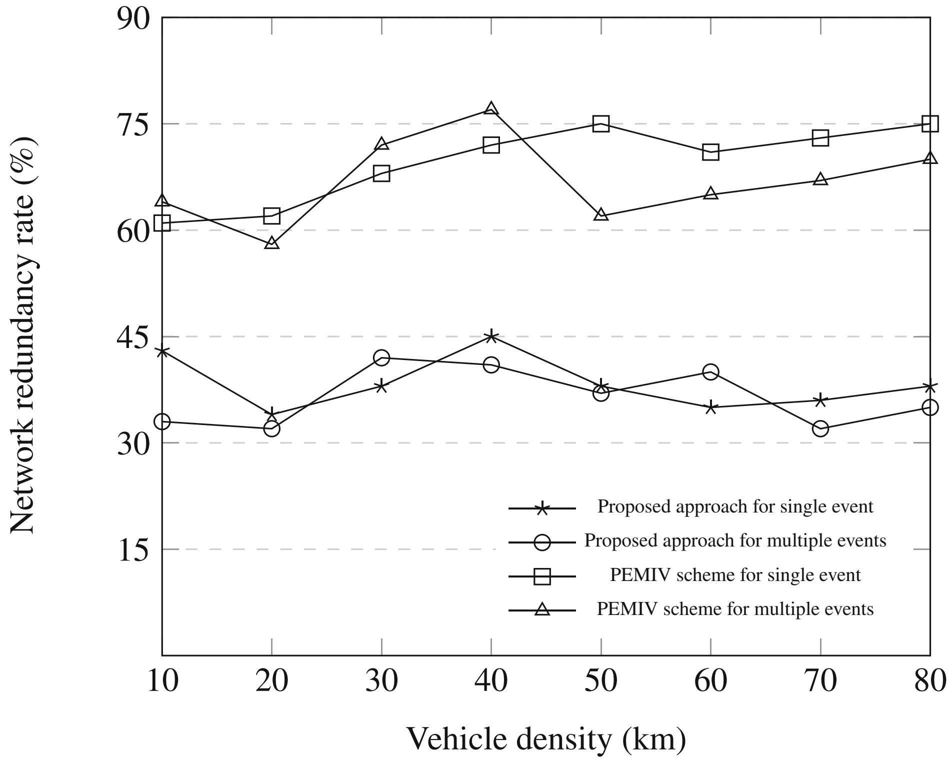

FIGURE 10 Network redundancy rate according to vehicle density.

TABLE 2 Evaluation results of proposed approach and PEMIV scheme.

No.	Performance parameter	PEMIV scheme (min–max)	Proposed approach (min–max)	Improvement
1	Packet delivery ratio (%)	32.3–59.6	57.2–79.1	20
2	Link lifetime (s)	45.2–63.3	58.1–76.4	13
3	Latency (s)	7.0–8.6	4.9–6.2	2.4
4	Dissemination efficiency (%)	20–60	45–70	10
5	Cluster stability (s)	12–13	22–24	11
6	RSU response time (s)	5.9–8.1	2.9–3.5	4.6
7	Routing overhead (ms)	62.2–76.4	45.1–45.8	31
8	Network redundancy rate (%)	59–72	32–42	30

Hence, it eventually maintains a lasting connection with the cluster members.

- Figure 8 shows the relation between the RSU response time and end-to-end communication distance between the source and destination. As distant communication involves more vehicular clouds, the RSU introduces an extra processing delay for data forwarding. Compared with the PEMIV scheme, the response time in the proposed approach is notably reduced by approximately 3 s, reducing the end-to-end delay.
- Figure 9 shows the relationship between the routing overhead and vehicle density at various mobility levels. The two-hop node selection and cluster stability substantially reduce the overhead, but it increases slightly with higher vehicle density, which slowly creates congestion. However, for vehicle densities of up to 40–60, the overhead remains constant, which affects the overall dissemination efficiency.
- Figure 10 shows the network redundancy rate according to vehicle density. This rate increases between 20 and 40 vehicles per kilometer but falls at higher densities because the THLLBA selects nodes with a two-hop distance. Thus, few nodes contribute to connection establishment, mitigating network redundancy by approximately 17% compared with the PEMIV scheme.

A summary of the comparison results is presented in Table 2. The PEMIV scheme and proposed approach values were obtained for vehicle mobility levels of 10–30 m/s.

6 | CONCLUSION

We propose an ANN-based intelligent data dissemination technique for efficiently forwarding safety information to a distant target vehicle in a VANET. Multiple agents are used to collect and coordinate a large amount of information generated in a V2I network. Internet services used in the proposed approach provide additional functionalities for fast data delivery. Vehicular clouds provide information at defined ranges, thus increasing the efficiency of data dissemination. The proposed approach may be more adaptable and easily used in real-time applications than similar solutions. In addition, it is more efficient than the PEMIV scheme in terms of data collection time, bandwidth utilization, and end-to-end delay. The outcomes of the proposed approach in terms of performance were as follows: packet delivery ratio increased by 15%, connection lifetime increased by 13%, end-to-end latency increased by 30%, distribution efficiency increased by 19%, and RSU response time increased by 20%.

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest.

ORCID

Ramesh B. Koti https://orcid.org/0000-0002-5832-314X

REFERENCES

1. M. Noor-A-Rahim, Z. Liu, H. Lee, M. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, *Poor, 6G for vehicle-to-everything (V2X) communications: enabling technologies, challenges, and opportunities*, Proc. IEEE **110** (2022), 712–734.
2. M. Hasan, S. Mohan, T. Shimizu, and H. Lu, *Securing vehicle-to-everything (V2X) communication platforms*, IEEE Trans. Intell. Veh. **5** (2020), 693–713. https://doi.org/10.1109/TIV.2020.2987430
3. N. Raza, S. Jabbar, J. Han, and K. Han, *Social vehicle-to-everything (V2X) communication model for intelligent transportation systems based on 5G scenarios*, (Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan), 2018, pp. 1–8. https://doi.org/10.1145/3231053.3231120
4. J. S. Warm, W. N. Dember, and P. A. Hancock, *Vigilance and workload in automated systems*, *Automation and human performance: theory and applications*, CRC Press, Boca Raton, FL, USA, pp. 183–200, 2018.
5. H. M. Furqan, M. S. Solaija, J. M. Hamamreh, and H. Arslan, *Intelligent physical-layer security approach for V2X communication*, arXiv Preprint, 2019, arXiv:1905.05075.
6. M. J. Sataraddi and M. S. Kakkasageri, *Connectivity and delay aware reliable routing in vehicular ad hoc networks*, (IEEE International Conference on Advanced Networks and Telecommunications Systems, Goa, India), Vol. **2019**, 2019, pp. 1–5. https://doi.org/10.1109/ANTS47819.2019.9117968
7. L. He, Z. Yan, and M. Atiquzzaman, *LTE/LTE-A network security data collection and analysis for security measurement: a survey*, IEEE Access **6** (2018), 4220–4242.
8. R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, *Evolution of V2X communication and integration of blockchain for security enhancement*, Electronics **9** (2020), 1338. https://doi.org/10.3390/electronics9091338
9. M. J. Sataraddi, M. S. Kakkasageri, G. S. Kori, and R. V. Patil, *Intelligent routing for hybrid communication in VANETs*, (IEEE 7th International Advance Computing Conference, Hyderabad, India), 2017, pp. 385–390. https://doi.org/10.1109/IACC.2017.0087
10. S. Panichpapiboon and W. Pattara-Atikom, *A review of information dissemination protocols for vehicular ad hoc networks*, IEEE Commun. Surv. Tutor. **14** (2011), 784–798. https://doi.org/10.1109/SURV.2011.070711.00131
11. T. Mahmood, *Data dissemination scheme for VANET using genetic algorithm and particle swarm optimization*, Int. J. Recent Technol. Eng. **10** (2021), 322–328. https://doi.org/10.35940/ijrte.A5970.0510121
12. G. Rathee, A. Khelifi, and R. Iqbal, *Artificial intelligence- (AI-) enabled Internet of Things (IoT) for secure big data processing in multihoming networks*, Wirel. Commun. Mob. Comput. **2021** (2021), 1–9. https://doi.org/10.1155/2021/5754322
13. S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, S. Tu, and I. A. Hameed, *EEMDS: an effective emergency message dissemination scheme for urban VANETs*, Sensors **21** (2021), 1588. https://doi.org/10.3390/s21051588
14. J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, *Big data analysis-based secure cluster management for optimized control plane in software-defined networks*, IEEE Trans. Netw. Serv. Manag. **15** (2018), 27–38.
15. E. Andrade, A. Santos, P. D. Maciel, and F. Matos, *Analyzing cooperative monitoring and dissemination of critical mobile events using VANETs*, Wirel. Netw. **27** (2021), 1981–1997. https://doi.org/10.1007/s11276-021-02551-z
16. E. Al-Ezaly, M. Abu-Elkeir, and A. Riad, *Collaborative vehicle location management service for enhanced hybrid reactive and proactive multicast in VANETs*, Arab. J. Sci. Eng. **42** (2017), 691–704. https://doi.org/10.1007/s13369-016-2289-x
17. M. A. Al-Absi, A. A. Al-Absi, R. Fu, K.-H. Kim, Y.-S. Lee, B.-G. Lee, S.-G. Lee, and H.-J. Lee, *Secure and efficient high throughput medium access control for vehicular ad-hoc network*, Sensors **21** (2021), 4935. https://doi.org/10.3390/s21144935
18. G. Rathee, S. Garg, G. Kaddoum, Y. Wu, D. N. Jayakody, and A. Alamri, *ANN assisted-IoT enabled COVID-19 patient monitoring*, IEEE Access **9** (2021), 42483–42492.
19. T. Zhong, B. Xu, and O. Wolfson, *Disseminating real-time traffic information in vehicular ad-hoc networks*, (IEEE Intelligent Vehicles Symposium, Eindhoven, Netherlands), 2008, pp. 1056–1061. https://doi.org/10.1109/IVS.2008.4621303
20. M. Ma, K. Liu, X. Luo, T. Zhang, and F. Liu, *Review of MAC protocols for vehicular ad hoc networks*, Sensors **20** (2020), 6709. https://doi.org/10.3390/s20236709
21. S. K. Basha and T. N. Shankar, *Fuzzy logic based forwarder selection for efficient data dissemination in VANETs*, Wirel. Netw. **27** (2021), 2193–2216. https://doi.org/10.1007/s11276-021-02548-8

22. M. De Felice, I. V. Calcagni, F. Pesci, F. Cuomo, and A. Baiocchi, *Self-healing infotainment and safety applications for VANET dissemination*, (IEEE International Conference on Communication Workshop, London, UK), 2015, pp. 2495–2500. https://doi.org/10.1109/ICCW.2015.7247551
23. S. A. Rashid, L. Audah, M. M. Hamdi, M. Abood, and S. Alani, *Reliable and efficient data dissemination schemes in VANET: a review*, Int. J. Electr. Comput Eng. **10** (2020), 6423–6434. https://doi.org/10.11591/ijece.v10i6.pp6423-6434
24. M. Ali, A. W. Malik, A. U. Rahman, S. Iqbal, and M. M. Hamayun, *Position-based emergency message dissemination for internet of vehicles*, Int. J. Distrib. Sens. Netw. **15** (2019), 1550147719861585. https://doi.org/10.1177/1550147719861585
25. X. Fan, C. Huang, J. Zhu, and B. Fu, *Replication-based data dissemination in connected internet of vehicles*, Wirel. Commun. Mob. Comput. **2019** (2019), 1–16. https://doi.org/10.1155/2019/2150524
26. A. K. Kazi, S. M. Khan, and N. G. Haider, *Reliable group of vehicles (RGoV) in VANET*, IEEE Access **9** (2021), 111407–111416. https://doi.org/10.1109/ACCESS.2021.3102216
27. A. F. M. Suaib Akhter, A. F. Shahen Shah, M. Ahmed, M. Moustafa, U. Çavuşoğlu, and A. Zengin, *Secured message transmission protocol for vehicular ad hoc networks*, Comput. Mater. Continua **680** (2021), 229–246. https://doi.org/10.32604/cmc.2021.015447
28. X. Fan, C. Huang, B. Fu, S. Wen, and X. Chen, *UAV-assisted data dissemination in delay-constrained VANETs*, Mob. Inf. Syst. **2018** (2018), 1–12. https://doi.org/10.1155/2018/8548301
29. M. S. Kakkasageri and S. S. Manvi, *Multiagent driven dynamic clustering of vehicles in VANETs*, J. Netw. Comput. Appl. **35** (2012), 1771–1780. https://doi.org/10.1016/j.jnca.2012.07.002
30. Y. S. Lee and S. Kim, *A proposal of novel design on the WAVE MAC algorithm with low-latency for seamless video surveillance in V2X environment*, Multimed. Tools Appl. **79** (2020), 16035–16049.
31. S. S. Mudengudi and M. S. Kakkasageri, *Agent based trust establishment between vehicles in vehicular cloud networks*, Int. J. Comput. Netw. Inf. Secur. **11** (2019), 29–36. https://doi.org/10.5815/ijcnis.2019.07.05

AUTHOR BIOGRAPHIES

Dr. Ramesh B. Koti completed his BE in Electronics and Communication Engineering and M.Tech. in Digital Electronics and Communication Systems at Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India. He completed his PhD in Vehicular Ad hoc Networks (VANETs) at VTU. He is an assistant professor in the Department of Electronics and Communication Engineering, Gogte Institute of Technology, Belagavi, Karnataka, India. He has published several research papers in national and international journals and conferences. His areas of interest include wireless networks, especially vehicular ad hoc and sensor networks.

Dr. Mahabaleshwar S. Kakkasageri is working as an associate professor of Electronics and Communication Engineering at Basaveshwar Engineering College, Bagalkote, Karnataka, India. He has 20 years of experience in teaching and research. His research interests include vehicular ad hoc networks, wireless networks, and the Internet of Things. He has published 2 patents, 57 papers at national and international conferences, 35 papers in national and international journals, and 6 book chapters. He coauthored the book *Wireless and Mobile Networks: Concepts and Protocols*, published by Wiley India. He is a reviewer and program committee member for many journals and international conferences. He was awarded "Seed Money to Young Scientist for Research" from VGST, Government of Karnataka, India, in 2015. As an advisor, he has helped seven PhD research scholars to obtain their degrees.

Dr. Rajani S. Pujar completed her BE in Electronics and Communication Engineering and M.Tech. in Digital Communications at Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India. She completed her PhD at VTU. She is currently an assistant professor in the Department of Electronics and Communication Engineering, Basaveshwar Engineering College, Bagalkote, Karnataka, India. Her research interests include wireless networks, signal processing, and the Internet of Things. She has published 2 patents and many research papers in national and international journals and conferences.

How to cite this article: R. B. Koti, M. S. Kakkasageri, and R. S. Pujar, *Artificial neural network for safety information dissemination in vehicle-to-internet networks*, ETRI Journal **45** (2023), 1065–1078. DOI 10.4218/etrij.2022-0203