Measurement: Sensors 29 (2023) 100878

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Design and Modelling of hybrid network security method for increasing security in vehicular ad-hoc network

Mohammed Zabeeulla [a,*], Arjun singh [b], Sudhir Kumar Sharma [c], Sanjay Pratap Singh Chauhan [d]

[a] Department of Computer Science Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka - 562112, India
[b] Department of Electronics and Communication, School of Engineering, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India
[c] Department of Electronics & Communication Engineering, Jaipur National University, Jaipur, India
[d] School of Computing Science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

ARTICLE INFO

Keywords:
Vehicular ad hoc network
Security
Denial of service
Authentication

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are becoming more commonplace as a means for cars to communicate and share data on things like traffic patterns, road conditions, and travel times and speeds. Therefore, one of the key issues facing academics now is ensuring data communication safety in VANET. There are several privacy-preserving verification techniques for VANETs. However, they do have complex calculations and safety issues. This research presented an operating platform for the 5G-based VANET architecture that combines Software-Defined Networking (SDN) with Self-Organizing Maps (SOM). The proposed system provides SOM and SDN-based network (SOM-SDN) solutions that will improve safety in two dimensions by spotting and stopping threats. First, this research examines the network's efficiency threats while considering Distributed Denial of Service (DDoS) threats. The suggested system's safety was then compared with current DDoS attacks. Additionally, the proposed method is strong enough to fend off typical assaults and maintain the communication information's secrecy, thanks to an examination of its security qualities. The efficiency comparisons' outcomes demonstrate the suggested procedure's light and effectiveness. Additionally, the suggested model using SUMO and NS-3 demonstrates how effective and useful the method is for VANETs. The proposed study shows a 92% improvement in performance, a 4% reduction in end-to-end latency, a 92% improvement in transmission outbound, a 98% improvement in packet transmission rate, and a 94% improvement in the enumeration of bounce compared to prior studies.

1. Introduction

There is a need to tackle the problem of the recent increase in road accidents and traffic violations by implementing VANETs to exchange safety messages, broadcast and inform passengers of real-time traffic details, and provide many more roadside services. VANETs are self-organization networks that are part of mobile ad hoc networks (MANETs). A VANET has a more dynamically changing network topology that requires a flexible clustering model to avoid connection failure [1]. It creates a network of smart vehicles that communicate with each other. The communication is established via both dedicated short-range communication (DSRC) and/or mobile cellular networks [2]. The communication methods depend on the components of this network, whether they are vehicles or fixed units called road side units (RSUs). A VANET encompasses vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [3].

As the number of automobiles on the road and the quality of wireless networks improve, studying VANETs has become an exciting new area of study. VANETs are a subtype of MANETs that use automobiles as mobile nodes and provide communication between nearby vehicles and between vehicles and roadside infrastructure. Moreover, VANETs' characteristics distinguish them from other networks. Furthermore, recent advances in transportation technology have led to the development of autonomous vehicles. Therefore, traveling will be made considerably easier, more productive, and safer due to VANET implementation. There are various challenges in deploying VANET framework including mobility of the vehicles, Dynamic topology, Minimum transmission delay, Connectivity of the network and optimal power usage.

* Corresponding author.
E-mail addresses: z.mohammed@jainuniversity.ac.in (M. Zabeeulla), ece.arjunsingh@dbuu.ac.in (A. singh), hodece_sadtm@jnujaipur.ac.in (S.K. Sharma), sps.chauhan@galgotiasuniversity.edu.in (S.P.S. Chauhan).

https://doi.org/10.1016/j.measen.2023.100878
Received 11 February 2023; Received in revised form 4 June 2023; Accepted 7 August 2023
Available online 8 August 2023

Technical issues with autonomous automobiles' security pose serious risks to the public. Among the many obstacles to the widespread adoption of autonomous vehicles is the need for improved safety features. VANET monitors traffic and relays information from nearby vehicles. Nodes in a VANET may be either permanently installed or temporarily relocated. This network aims to make drivers safer by facilitating the secure exchange of information concerning traffic incidents and vehicle collisions. However, automobiles on the system may not transfer information, submit fraudulent requirements, or try to break security in other ways. Specifically, if vehicles equipped with VANETs travel down the road, it design restricts their ability to communicate with one another. Therefore, future vehicle positions can only be readily anticipated if it is possible to collect road data [4]. When it comes to keeping passengers and driving safely on the road, VANETs are invaluable [5]. At the same time, the arrival of 5G wireless services would enhance the current connections between automobiles, the performance of vehicles, the user experience throughout the trip, etc. To provide superior online communication amongst road vehicles, ITS relies on developing VANETs and 5G networks [6].

5G mobile networks are necessary to satisfy the application demands of ITS because of the increased capacity and decreased latency communication they provide [7]. However, because of the limited spectrum availability, future 5G networks may probably be unable to handle autonomously the constantly changing information in vehicles. Due to ongoing improvements in VANET technology [8], it will soon be possible to offer a wide range of facilities, including observation, health, traffic flow monitoring, IoT-based promotion, etc. VANETs are extremely difficult to coordinate due to their unique properties. VANETs are tasked with efficiently providing a variety of services with varying requirements for quality. There is a growing need for programmatic network frameworks to help VANETs enhance collaboration across underlying heterogeneous networks, coordinate the allocation of resources, and efficiently control an enormous amount of mobile nodes equipped with a wide variety of smart devices [9].

The SDN strategy that separates network administration from information exchange will be crucial to future network design. The network design of the next generation of VANETs will rely heavily on software-defined networks supported by 5G technology. The capacity to programmatically deploy resources and manage networks is a key feature of software-defined networking made possible by separating the data and control planes. Virtualization of network resources and application personalization in response to user demands is generally recognized as a key approach in 5G networks. Intelligent transportation systems that utilize VANETs for autonomous driverless systems and automobile driving assistance systems are often organized using a self-organizing map [10]. Vehicles were clustered into VANETs based on differences in travel directions and final destinations gleaned from their periodic messages. The constructed automobile mostly exchanges information with and processes commands from other vehicles in the same VANET. VANET may benefit greatly from the ability to anticipate the next movement drivers choose at each intersection in a road network. Several VANET services that rely on the Global Positioning System (GPS) suffer challenges due to obstacles like trees, tall buildings, and tunnels [11].

A vehicle's future travel direction may be predicted using a global positioning system. Self-organizing mapping is used to recover vehicle movement patterns by grouping vehicles' paths while in motion [12]. The driver will utilize these patterns to determine the next step in the sequence of movements at the next intersection. The 5G VANET system integrates software-defined networking to facilitate data exchange and coordination across base stations for more effective and flexible clustering. VANET uses software-defined networking [13] to manage network-wide communication. In vehicle networks, routing protocols assist in regulating all communication. The importance of routing protocols in maintaining the VANET's safety, confidentiality, and interaction has grown in parallel with the system's popularity. SDN technology is the best way to fix this problem. Using network traffic statistics, a self-organizing map is trained for detection [14]. After the first training data set, it continuously identifies the features of fresh arriving traffic and classifies it accordingly. It has been used for surveillance because of its versatility and ability to adjust to new conditions. The use of an SDN in VANETs has reduced the complexity of the operation of the networks themselves. The research developed a hybrid strategy, integrating SDN and SOM, to improve the safety of automotive ad hoc networks.

The research adds new information since, to our knowledge; no previous studies have combined SDN and SOM for VANET under the 5G framework, as shown in the following overview.

- For VANET, a novel architecture has been developed that merges software-defined networking (SDN) with service-oriented networking (5G network).
- To detect spoofed Internet Protocols (IP), a database of IP packet binding is maintained, and all packets obtained for a given IP address are analyzed by comparing the number of messages per second to a threshold.
- In conclusion, the outcomes show that the proposed method may increase security and, in turn, can affect and improve end-to-end latency, packet loss, and throughput.

2. Literature Review

A trustworthy model can manage risks and uncertainties emerging from faulty data in moving vehicles. However, VANET may be disrupted by impediments that can be moved or are immovable and by faulty, incomplete, or erroneous data acquired by vehicles. Soleymani et al. [15] offered a Fuzzy Trust Model (FTM) for the vehicle network grounded in past experience and probable future outcomes. The suggested trust model runs through a battery of safety tests to verify the authenticity of data obtained from approved cars. In addition, fog nodes are used as a measurement tool for precisely an event was located. The experiments' findings show that the suggested method not only discovers attackers and malfunctioning nodes but similarly overcomes the inaccuracy and uncertainty of automobile information in both sightline and non-sightline scenarios.

The development of VANET technology has brought renewed focus to the concept of clustering. Various clustering methods have been presented in the literature, with the majority aiming toward cluster stability on the assumption that all nodes can be relied upon. Nevertheless, due to the critical role that cluster heads play, the determination of a hacked node as a cluster head may have far-reaching consequences that represent a major danger to the security and resilience of the network. Oubabas et al. [16] offered a novel method that uses a mixed algorithm to combine stability and trust criteria to choose reliable cluster heads. Unlike previous studies, the work on trust management considers both the vehicles' communication capacities and the trustworthiness of the data they share to maximize safety and dependability. Based on the simulation results, it is perfect that the existing method is greater than the most recent Clustering Protocols (CP) described in VANET, as it greatly increases cluster stability and guarantees greater vehicle collaboration and accurate data exchange.

Establishing a reliable means of communicating urgent information outside a dangerous area is difficult. In VANETs, the primary routing goals are maximizing the data rate, minimizing routing latency, and avoiding congestion. Furthermore, VANET networks may be targeted by a wide range of malicious activities. Overhead delay is caused by an algorithm employed in traditional VANET systems to detect assaults at confirmation time. To identify DoS assaults before the confirmation time, the (*P*-Secure) method is proposed in this work. It improves the safety of VANETs while decreasing processing times. Fotohi et al. [17] proposed a *P*-Secure method that is more effective in simulations than the OBU model VaNET method in terms of packet delivery ratio, elapsed time between transmissions, throughput, and the percentage of dropped

packets.

Vehicular ad hoc networks provide unique routing challenges owing to characteristics like node mobility and intermittent wireless connectivity. In addition, these networks are exposed to a broad range of attacks because of the characteristics mentioned above, requiring the design of a verification technique among the source and destination critical. Azhdari et al. [18] provide an Authentication-capable Fuzzy Logic-based Routing (AFLR) approach for VANET. As a first step, a strategic method is used to group automobiles together. The suggested technique distinguishes between two distinct categories of information packages such as urgent and regular. Phase 2 details the various data packets' unique path-finding procedures. Keep in mind that there is a clear separation between insecure and secure data packets. An authentication mechanism is not present in a simple data packet. The authentication technique of secure data packets is based on Message Authentication Code (MAC) and geometric key cryptography. The suggested technique has been shown to perform better than others in terms of throughput, Packet Delivery Rate (PDR), Packet Loss Rate (PLR), and Round-Trip Delay (RTD).

Liu et al. [19] proposed a blockchain-based security strategy in this work, with two distinct blockchains built from Road Side Units (RSUs) and Certificate Authorities (CAs). The suggested safety approach aims to do many things, including identifying harmful nodes and detecting fraudulent communications based on criteria like sender node reputation and messages' time and distance efficiency. In addition, the RSU blockchain currently includes an incentive mechanism for RSUs to engage in pro-social practices. Extensive simulations demonstrate that the proposed methodology outperforms prior approaches in spotting fraudulent communications and locating harmful nodes. At the same time, it helps keep personal information secure and makes transportation networks more effective.

Attacks on forwarding devices and vulnerabilities in the control plane and communication channels are only a few examples of the security issues plaguing SDNs. The existing research provides an evidence-based blockchain system as a first line of defense against such attacks. The system can potentially reduce assault probability by as much as 99%. Quality of Service (QoS) decreases across the board as measured by end-to-end lag, power consumption, and data transfer rates in a network. Choudhary et al. [20] offered a machine-learning approach for optimizing blockchain parameters in a QoS-aware fashion that will help enhance these parameters while keeping the network secure. This machine learning technique draws inspiration from Q-Learning and works to mitigate the negative impact blockchain activities have on the Quality of Service (QoS) on VANETs. Since sidechain-based blockchain applications are quicker, more secure, and less sophisticated than single-chain implementations, it forms the basis of the underlying network. Based on the results, the suggested architecture may reduce end-to-end latency by 20%, power consumption by 18%, and total transmission by 40% compared to current blockchain-based SDN VANET solutions.

Integrating an SDN into VANETs has streamlined the operation of the networks altogether. The proposed research combines SDN with SOM to improve the safety of automotive ad hoc networks.

3. Proposed Methoology

Designed to fulfill the requirements of the next generation and adapt to their expectations, the suggested design is a radical change from the standard VANET. Key components of the proposed system are outlined below: Fig. 1 shows The SDN VANET Architecture.

3.1. Evolved node base controller (ENBC)

The next-generation 5G system will include ENBC. In this design, ENBC and the SDN controller work together. With these two elements together, an SD base station may be constructed for remote monitoring and administration of mobile devices. The evolved node base controller is responsible for directing traffic flow, enforcing network regulations, ensuring network security, and monitoring network integrity in a VANET.

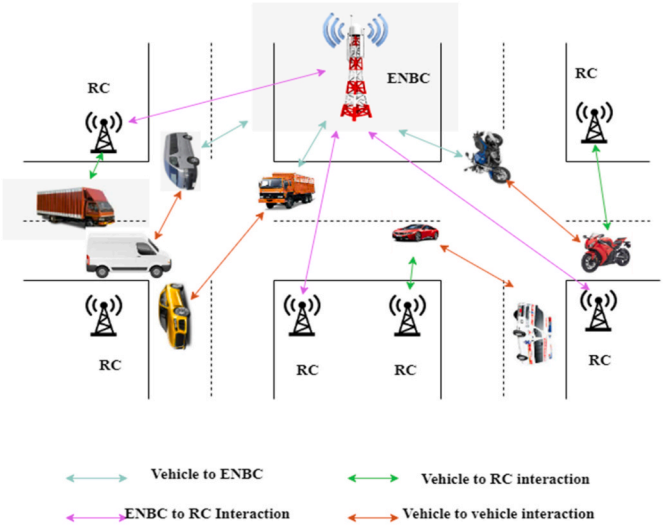

Fig. 1. The Sdn Vanet architecture.

3.2. Roadside controller (RC)

This smart controller guarantees fast processing, scalability, rule enforcement, and adaptability by employing microcells for direct connections to cars. The RC and the ENBC work together to police security and oversee traffic. Cooperatively, they oversee the vehicle's control plane, data plane, and security plane.

3.3. Connected smart wireless nodes (CSWN)

Indicated by these nodes are mobile devices that may act as wireless hosts and facilitate communication with other vehicles. In addition, regional control centers collect crucial data and relay it to local agents in automobiles to handle security.

In a traditional VANET architecture, each vehicle uses its special set of mobile communication units to pair up with the RSUs. The architecture uses this method to transpose data collected through wireless methods into a useful form for load balancing and security. In addition, the technology's control plane uses brief-range wireless communication like WiMAX/LTE. As a result, the data plane may gain from the increased transmission and lowered communication costs without sacrificing wireless dependability.

3.4. Attack foresight, protection, and identification

3.4.1. Acknowledgment and verification

The suggested method offers a worldwide authentication mechanism to stop impersonation attacks on different parts of the network. At first, each RC has to be approved and verified by the ENBC. Here, the ENBC is seen as a reliable source. The ENBC and the RC must verify each vehicle before it can be stored in the RC's local database and given its official seal of approval. A demand for verification is sent to the RC whenever a new vehicle attempts to join VANET. Using a response protocol, the RC sends this demand to the ENBC\that must first validate the RSC; the demand is included to reduce the number of communications transferred between the parties involved. The protocol uses the request and answer to minimize communication. The credential is then issued to the vehicle and stored in the local RC database, the ENBC's evolved database. Once the RC has verified a vehicle, the ENBC will only get a

reference to it whenever it makes a subsequent connection request. While ENBC or RC can generate keys, only evolved NBC can generate certificates.

As the vehicle crosses from one RC's domain to another, the RCs can carry out mutual verification utilizing stored certificates, with the former confirmed by ENBC during the transfer. The old RC's first handover request is generated and sent to the new RC. Consequently, later the succeeding authentications stage concludes, and the outgoing RC will provide the incoming RC with access to the vehicle credentials. Similarly, the vehicle will be appropriately authorized when it seeks a connection to the new RC. At the end of the transfer process, the new RC will inform ENBC of the automobile's current position. The ENBC must verify the new RC before the update may be established. When enabled on ENBC, the Acknowledgment and Verification (AV) module creates a record of verifications and restrictions on each RC, enforcing the network's overarching basic authorization requirements.

3.5. Attack Identification and prevention

Many of the hazards in a VANET come from compromised nodes or malevolent vehicles. DDoS attacks are the kind of attack that must be mitigated. These attacks operate by overwhelming the system with traffic destined for random RCs that causes the ENBC to become overloaded and disrupts the system opinion at the regulator level that, in turn, slows down the sending procedure in the data plane or even prevents the RCs from providing their services altogether. IP phishing is another attack that conceals the true attacker's identity by imitating their network's IP address. The suggested method in this research seeks to identify DDoS assaults launched by automobiles at different RSCs or other vehicles. The proposed system is outlined in this section.

- ➢ Collecting data packets directed at a certain IP address, then using that address's packets-per-second count to determine whether or not it's over or below a given limit.
- ➢ Keeping track of IP addresses and other Internet data to identify instances of IP address spoofing. Whenever an attack is discovered, a warning is sent along with the attacker's Source Identifier/Internet Protocol address.
- ➢ As soon as IP spoofing is detected, a traceback mechanism is started to stop the attack at its source.

The following diagram sums up the procedure in its entirety. A detailed process diagram is shown in Fig. 2.

3.6. Each procedure is detailed below

3.6.1. Within the range of the automobile

The controller can monitor all connected vehicles according to the IP detection binding's easy setup. A warning is directed to the server's safety module if the server receives a package from a resource that does not adhere to the switch's binding standards. The security agent in the vehicles sends the packet headers of the different phishing data to the detection area via the protection plane. The source id of fraudulent messages that violate the binding rules is changed at the switch level to apply assault traceback regulations. Only those special packets should reach the security module.

When the controller receives updated packets, it sorts them by signed IP addresses. After receiving the updated signed packets, the controller can determine that RC and the vehicle were responsible for the assault. Only when the total number of these packets reaches the threshold value are these treated as part of a DDoS assault; otherwise, these are treated as unwanted traffic and dropped. On the RSC/Vehicle side, preventative measures will be taken in any scenario. When a denial of service assault through Internet Protocol spoofing is detected, the request to implement an IP/Identity blocking standard across all switches or a single port is sent to the controller using a REST Application Programming Interface.

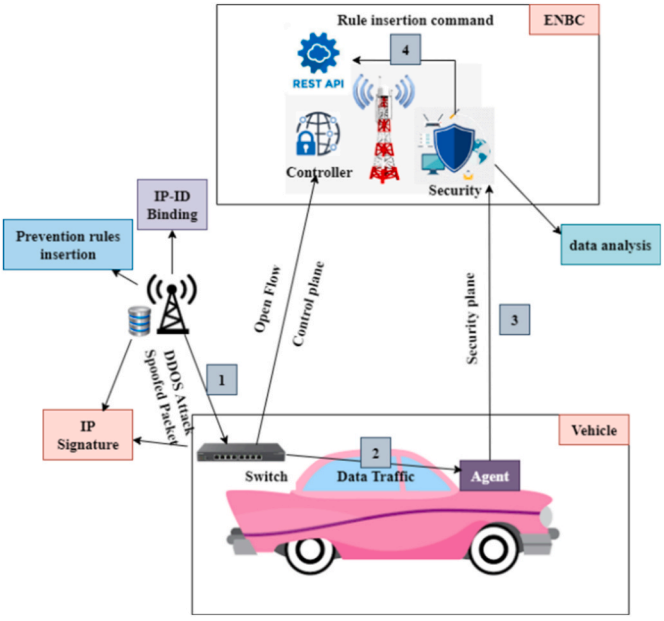

Fig. 2. Attack identification and prevention process.

As has been shown before, when a set of packets violates a policy, an alert message is generated based on the invariances found in the packet in messages. When processing power has to be moved closer to the consumer, as in fog computing, reaction times and latency may be improved. This architecture's attack detection and prevention techniques must be incredibly fast when dealing with fast vehicles. Therefore, it is suggested to include the security functions of the security module in the small cell, providing the RC with the processing power it needs. The adaptive control approach is a risk-free procedure. It reveals the issue and requires the enclosure of the RCs to increase transmission power if even a single RC or the ENBC station fails. As a result, the transmission range for cars must be increased so that they may connect to these RCs in a dispersed fashion until the problem is determined. The suggested technique prevents harmful sites from tainting the operator's view of the overall system by spoofing the IP addresses. It also predicts assaults in real-time utilizing minimum controller resources and with the least amount of design. Fig. 3 Shows the Diagrammatic Representation of Attack Detection.

The suggested system's primary objective is to provide a hybrid method of improving VANET security via using 5G networks. For example, the figure below depicts a VANET network diagram using SOM and SDN: Fig. 4 Shows the An Open Flow Switch Implementing SDN and SOM in a VANET Network.

The first phase is the creation of a VANET consisting of many nodes that will incorporate RC and moving cars. The automobile acts as a future 5G network component known as ENBC. Integrating the evolved node base station with SDN is the first step in developing a Software-Defined Base Station (SDBS) for wireless network management and control. The ENBC is the brains behind the VANET and is in charge of maintaining security, directing policy, ensuring uniformity, and directing traffic. To provide fast handling, scalability, instruction administration, and tractability, the RC is a smart microcell organizer for direct communication with automobiles. The RC and ENBC work together to police security and control traffic. They oversee the wireless network's control plane, data plane, and security infrastructure (vehicles) as a group. The open flow switch is used in the second phase to implement SOM and SDN on the VANET network. The open flow switch consists of a switch and a controller. It is expected that the SDN integration would mirror the framework described in the research 5G SDN-based VANETs.

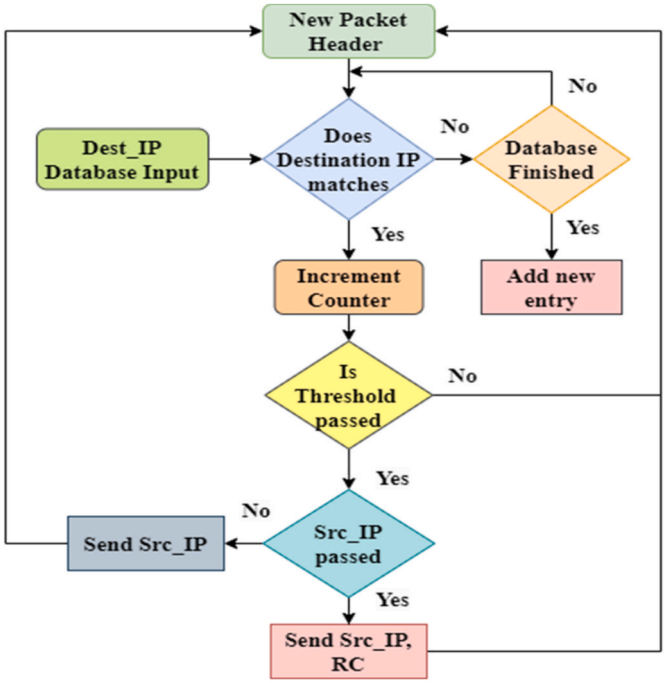

Fig. 3. Diagrammatic representation of attack detection.

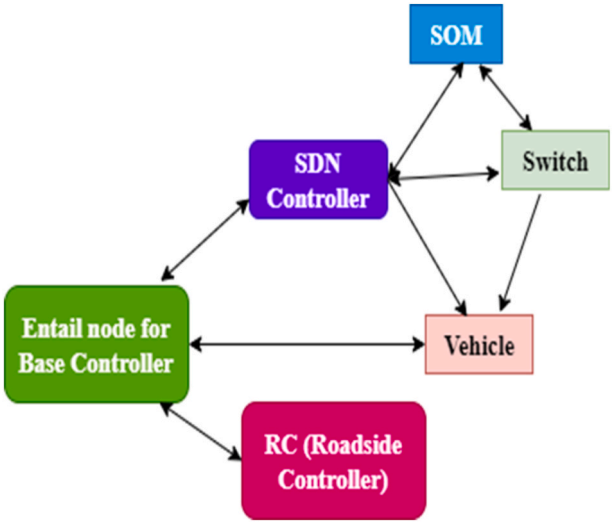

Fig. 4. An open flow switch implementing Sdn and Som in a Vanet network.

3.7. Algorithm for SOM

SOM is an unsupervised learning-based DM approach. The SOM method rearranges the incoming data and represents it in a node grid or map that is a low-dimensional space. The self-organizing map facilitates the construction of a low-dimensional representation of the high-dimensional input data. Different nodes react differently to input patterns when a network is trained using SOM. The section below explains each of the SOM algorithm's steps.

3.8. SOM algorithmic steps

Step 1: First, a vector is initialized with either static or randomized values for each map node.
Step 2: When an input vector is provided, the Euclidean Distance (ED) to each cluster in the plan is calculated.
Step 3: The closest cluster to the input terminal is the one that will be used as the Best Matching Unit (BMU)
Step 4: The BMU's nearby radius is calculated to save time.
Step 5: The nearby nodes of the vector are modified according to the following equation such that the result strongly matches the input vector in equation (1):

$$Z(q+1) = Z(q) + QP(q) * PE(q) * (U(q) - Z(q)) \tag{1}$$

In this case, $QP(k)$ represents the learning rate that must decay naturally with time. Distance from Current Location to Best Matching Unit, denoted by $PE(k)$. As a node draws closer to the Best Matching Unit, the greater the unit's influence on that node's vector.

Step 6: The process described in Step 2 should be repeated several times.

The system may be configured dynamically using SDN, allowing faster reaction times and more accurate attack detection. In Fig. 2, a hybrid approach to DDoS detection is shown in detail. The controller creates a normal level throughout its computational period by computing the correlation between all the characteristics collected from the flows received by the switches and controller using equation (2). Furthermore, the same correlation metric may be used to establish a typical experimental amount of observed traffic. An alert will sound, indicating an assault has occurred if the perceived traffic difference between the baseline and the experimental level is greater than the dynamic threshold value.

$$R = 1 - \sum_{l=1}^{m} \frac{\left|A_{(c,d)} - B_{(c,d)}\right|}{\left|\left|\varepsilon_{A_{(c,d)}} - \beta_{A_{(c,d)}}\right| - A_{(c,d)}\right| + \left|\left|\varepsilon_{B_{(c,d)}} - \beta_{B_{(c,d)}}\right| - B_{(c,d)}\right|} \tag{2}$$

Where,

$$\varepsilon_{A_{(c,d)}} = \sum_{l=1}^{m} A_i$$

$$\beta_{B_{(c,d)}} = \sum_{l=1}^{m} B_i$$

$$\beta_{A_{(c,d)}} = \sqrt{\left|\varepsilon_{A^2_{(c,d)}} - \left(\varepsilon_{A_{(c,d)}}\right)^2\right|}$$

$$\beta_{B_{(c,d)}} = \sqrt{\left|\varepsilon_{B^2_{(c,d)}} - \left(\varepsilon_{B_{(c,d)}}\right)^2\right|}$$

Identifying the critical value:
Given the complexity of real-time data, these datasets are highly valued by attack-based software since the assaults have a relatively straightforward structure and kind. To determine an attack threshold for our article, we conducted experiments using data from simulated SDN networks. To identify DDoS assaults in real time over short periods, the dynamic threshold is computed using a time sequence-based technique (3).

$$K_1 = J'_{(l,k-1)} + \gamma.\beta_{J_{(L,K-1)}} \tag{3}$$

The constant γ in equation (3) is a close approximation to the experimentally determined coefficient. equations (4)–(6) are used to determine the mean value of entropy J, and the standard deviation β over a time interval d.

$$\overline{J_{(c,d)}} = \frac{1}{d} \sum_{l=1}^{d} J_{(c,d)} \tag{4}$$

And

$$\beta_{J_{(c,d)}} = \frac{1}{d}\sum_{l=1}^{d}\left(J_{(c,d)} - \overline{J_{(c,d)}}\right)^2 \tag{5}$$

$$J_{(c,d)} = -\log\frac{A_{(c.\ d)}}{\sum_{l=1}^{m} A_{(c,d)}} + \rho_{(c,d)} \tag{6}$$

$$\rho_{(c,d)} = \left|\log\frac{a_{(c,d+1)}}{a_{(c,d)}}\right|, a_{(c,d)} \geq a_{(c,d+1)} \tag{7}$$

$$\rho_{(c,d)} = \left|\log\frac{a_{(c,d)}}{a_{(c,d+1)}}\right|, a_{(c,d)} \leq a_{(c,d+1)} \tag{8}$$

γ is an experimental parameter that has a significant impact on attack detection precision when used in dynamic threshold calculations. Adopting the best value for γ is a subjective task that depends on several factors; therefore, it is important to take these interactions into account when making a final decision. The capability to detect the attacks is linked to several other factors. Furthermore, there should not be a large number of time slots, and a reduced computational burden should be associated with producing low false alarm rates. It means that the True Positive Ratio (TPR) of 100 defines perfection in the study. While optimizing TPR is the top priority when choosing γ, normal flow could be mistaken for an attack that unintentionally boosts FPR. The best time period is one in which the FPR value is typically lower than in other periods while taking the precise for each optimal time into account. Once an attack flow has been detected, it is sent to subsequent ML classification steps to improve detection accuracy further. Before sending data to ML classifiers, however, it destroys the portion of normal traffic flow that could be correctly detected. Additionally, the accuracy of ML classification algorithms improves.

4. Results

The KDD CUP 99 dataset is extremely difficult due to its vast size, high redundancy, many variables (both numerical and categorical), and the skewed target variable. Nevertheless, it's a common resource for research on intrusion detection. In 1999, during a DARPA-sponsored event held at MIT's Lincoln Laboratory, the database was first developed via the simulation of many assault scenarios and the extraction of characteristics. There are 4,898,431 records in the training dataset. High repetition (78%), however, means that only 1,074,992 data points are original. There are 311,029 samples in the test dataset.

4.1. Analysis of performance rate

Accuracy, precision, and recall metrics were used to assess the effectiveness of the suggested method. When a model successfully predicts the positive class, then indicates that it has produced a True Positive (TP). For a model to produce a True Negative (TN), it must correctly forecast the undesirable class. A False Positive (FP) occurs when a typical forecasts an optimistic class but does so inconsistently with the criteria. When a model predicts a negative class that does not meet the criteria, it produces a False Negative (FN). Table 1 provides the formula for determining the parameters. Table 1 Shows the Performance Rate Parameters.

Table 1
Performance rate parameters.

Parameters	Formulas
Recall	$\frac{TP}{TP+FN}$
Precision	$\frac{TP}{TP+FP}$
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$

We evaluate the effectiveness of the suggested security mechanism (i.e., the SOM scheme) about two baseline algorithms. We model the performance metrics (i.e., recall, accuracy, and precision) in a scenario with an arbitrary number of vehicles. Fig. 5 below show the results of the simulations. We assess the SOM system fares under a range of vehicle densities. In Fig. 5, it is clear that the SOM is superior to both CP and FTM in terms of accuracy, precision, and recall. According to the results shown in Fig. 5, the MGHSOM scheme has the potential to improve the accuracy of both the CP and the FTM by 3722.3% p and 4279.9% p, respectively. In addition, the effectiveness of the MGHSOM is analyzed in a realistic assault scenario. As part of the KDD CUP dataset, researchers randomly modify the attack pattern duration and the value of the basic and content features by 15%–60%. Fig. 5 exhibit simulation results demonstrating the SOM scheme's superior performance compared to the other two models. Fig. 5 demonstrates that the SOM scheme outperforms the other two algorithms in terms of accuracy by a margin of 16.83% *P*-Secure and by 39% for CP.

Fig. 5 compares the performance analysis of the proposed research to those of the existing research.

4.2. Delay from beginning to end

$$\text{End to end delay} = \frac{\sum_{i=1}^{k} D_i}{k} \tag{9}$$

In equation (9), D_i is the average delay from the beginning to end of packets of an ith vehicle, and k is the vehicle number.

Attack Alert Message via SOM model time spent in transit, measured in EED units. While SOM's improved mobility use cases are generally positive, it may cause alarm messages to arrive late. Delay-Tolerant Networks (DTNs) are favored for usage in VANETs due to their ability to minimize EED by allowing for packet delivery delays of varying durations. Fig. 6 demonstrates the SOM method outperforms CP and FTM. Fig. 6 shows the consistent increase of 200 automobiles every increment. The table numbers also show that when the number of cars increases, the average EED per packet sent by SOM decreases steadily. It is clear from the data that there has been no consistency in the EED levels reported and that the number of cars has increased dramatically. It is estimated that the median EED delay at the SOM is close to 1%. CP and *P*-Secure take much longer than the SOM method (respectively, 62.9% and 6.3% longer). The EED is more than 63.7%, which significantly improves the CP schemes. Accordingly, the SOM method outperforms both AFLR and

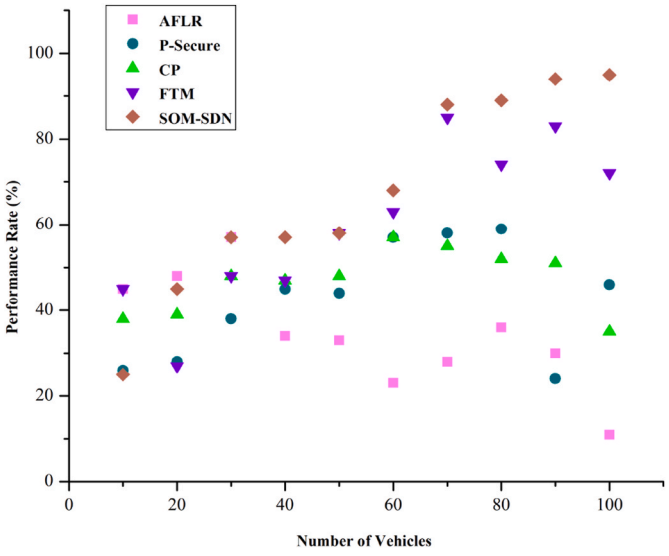

Fig. 5. Performance rate comparison results.

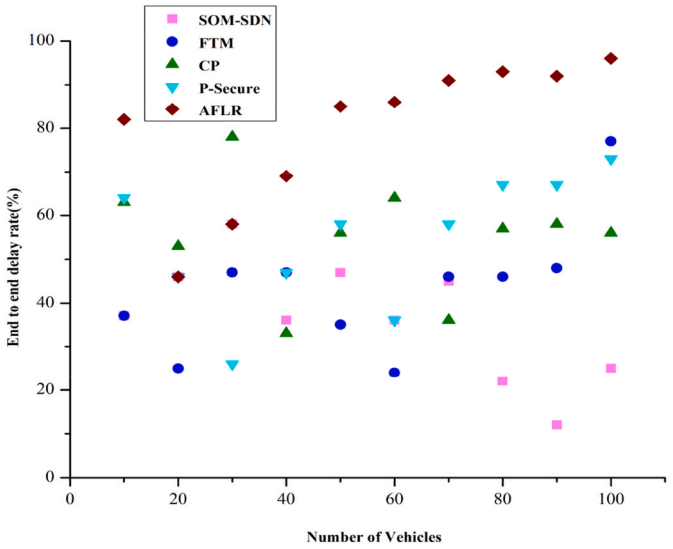

Fig. 6. End-to-end comparative results.

CP in these simulations. SOM outperforms the other two methods because it requires much less data about the network and route discovery process, reduces network overhead, and makes it an ideal case study for dynamic and scalable networks.

Fig. 6 compares the proposed research's end-to-end latency to those of the existing research.

4.3. Transmission outgoing (bits/sec)

$$\text{Transmission outgoing} = \frac{\text{Total amount of data}}{\text{Total time to data transfer}} \tag{10}$$

The most important parameter in SOMs, in terms of both performance and data flow, is the selection of the optimal route calculated by utilizing equation (10). However, with VANETs, the connection lifetime depends on several criteria, including vehicle transmission range, vehicle density, distance between adjacent vehicles, and vehicle transmission range. It's difficult to maintain connection stability with these values. The average connection duration was used due to the importance of many elements in determining the total link establishment time. The number of cars increases steadily, by 200 at each stage. Results find that the SOM provides a much more reliable and constant connection duration of 30.1% and 8.1%, respectively than CP and FTM. However, the connection time in CP is 26.1% longer than in FTM. Thus, with an increase in the number of cars, SOM maintains link consistency, and very little change is noticed in the average link values. However, the other two schemes, *P*-Secure and AFLR, undergo an unanticipated shift in link length with an increase in vehicle density and reduced stability, as noted in Fig. 7. It is clear from the comparative findings that the suggested SOM is more productive from a time perspective but at the expense of smaller packets. The suggested method identifies and favors more constant and reliable routes between data transfer endpoints, including periodic intervals with high connection stability.

Fig. 7 compares the outgoing transmission analysis of the proposed research to those of the existing research.

4.4. The successive rate of packet transmissions

$$\text{packet delivery rate} = \frac{\sum \text{number of packet received}}{\sum \text{number of packet sent}} \tag{11}$$

Actual data packets received as a fraction of the total data packets sent constitute the PDR in equation (11). The PDR grows with the

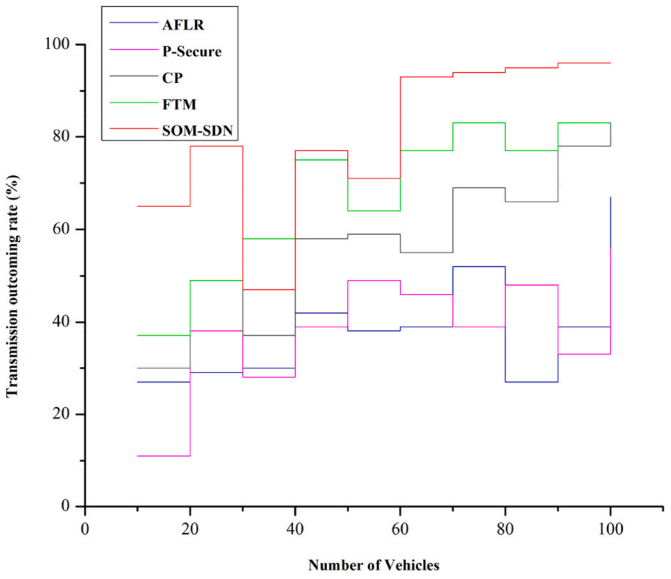

Fig. 7. End-to-end comparative results.

number of nodes, as seen in Fig. 8 at 100 nodes; it reaches its maximum value. In contrast to EAODV and other methods, the SOM approach offers a greater PDR rate for each node inspection. Changes in the state of the network are the root cause of PDR variations.

Fig. 8 compares the packet delivery rate of the proposed research to those of the existing research.

5. Enumeration of bounce

$$\text{Routing information protocol metric} = (\text{Hc} \times \text{W}) + \frac{(\text{D} \times (1 - \text{W}))}{\text{k}} \tag{12}$$

In equation (12), *Hc* hop count, *W and* $(1 - W)$ weights, *D* is the distance, and *k* is the factor of normalized distance to the hops.

As seen in Fig. 9, the vehicle density is modified when the number of cars in a certain area reaches 100. Even if the number of automobiles on the road has grown, the suggested SOM algorithm has become much less burdened. The SOM plan reduces the amount of overhead and load by

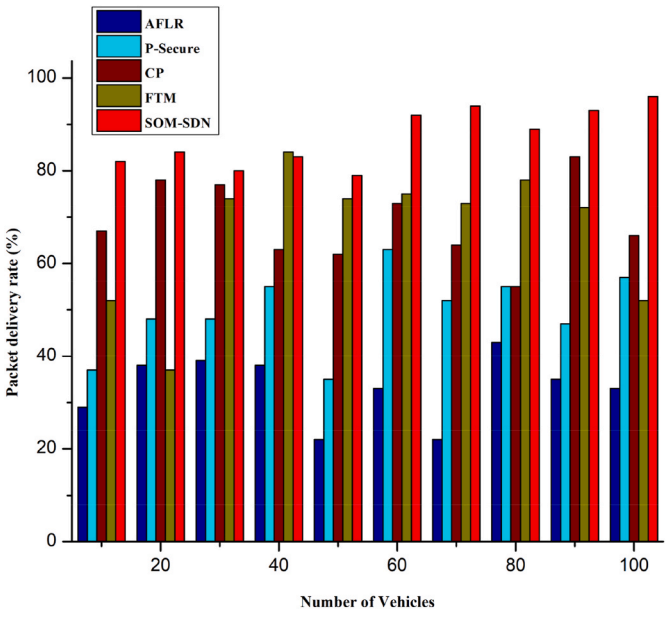

Fig. 8. Packet delivery ratio comparative results.

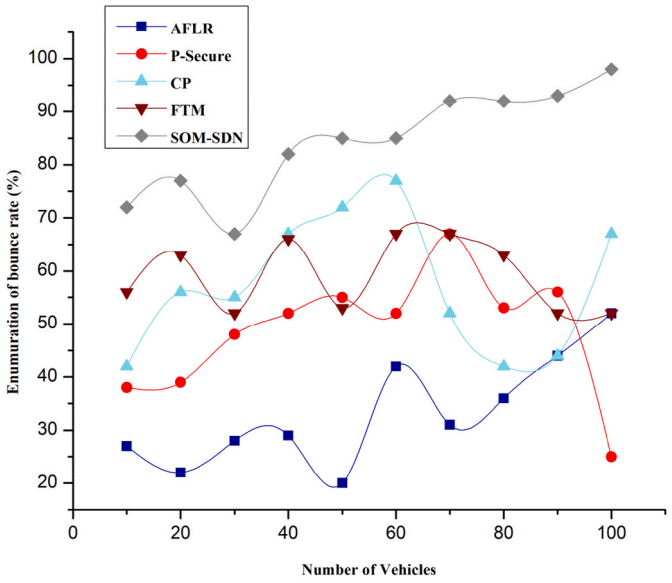

Fig. 9. Enumuration of bounce rate comparative results.

the increasing vehicle density. However, the other two algorithms have rising overhead as the number of cars increases. Fig. 9 shows that whereas SOM has a negligible amount of overhead, the routing overhead experienced by CP and FTM is 31.3% and 16.2%. Therefore, SOM is more effective than the other two procedures by 32.3% and 18%, respectively. The technique was developed to recognize routes and choose the most consistent and trustworthy path for data packet transfers that drastically cut down on Route Requests. The overhead involved in determining a path for transferring data is reduced, reducing the number of path rejections and control messages. That takes time for the values of routing overhead to converge on a minimum and an increase of 200 in vehicle density at each stage. Still, the *P*-Secure and AFLR techniques make a remarkable shift in routing overhead. Based on this evaluation, the SOM approach is superior to the other two systems.

Fig. 9 compares the enumeration bounce analysis of the proposed research to those of the existing research.

6. Conclusion

The research proposes a new, efficient method for securing VANET, which employs SOM with SDN in a 5G scenario instead of having to build up control planes, avoiding information latency and regulator overload. Potentially resolving the most pressing security concerns in VANETs, the suggested solution has several potential applications. First, the new security plane is the basis for a new network security solution that can identify and avert threats. Second, the network's susceptibility to performance degradation is examined in this paper. Second, the proposed system offers network solutions based on SOM and SDN to enhance security in parallel dimensions via the detection and prevention of attacks. Third, the research considers DDoS attacks, analyzing the dangers to a network's performance. The security of the proposed solution was then analyzed and compared to modern DDoS assaults.

Furthermore, research into the suggested method's security properties reveals that it is robust enough to withstand common attacks and preserve the privacy of communication data. The proposed study shows a 92% improvement in performance, a 4% reduction in end-to-end latency, a 92% improvement in transmission outbound, a 98% improvement in packet transmission rate, and a 94% improvement in the enumeration of bounce compared to prior studies. SDN combined with deep learning to detect DDOS attacks in VANET is the future direction of the suggested study.

Funding statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data.

References

[1] Junwei Liang, Jianyong Chen, Yingying Zhu, Richard Yu, A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position, Appl. Soft Comput. 75 (2019) 712–727.
[2] A.M. Ivanov, S.S. Shadrin, Development of autonomous vehicles' testing system, in: IOP Conference Series: Materials Science and Engineering, vol. 315, IOP Publishing, 2018, 012011, 1.
[3] Somayeh Mokhtari, Nima Nouri, Jamshid Abouei, Avid Avokh, Konstantinos N. Plataniotis, Relaying data with joint optimization of energy and delay in cluster-based UAV-assisted VANETs, IEEE Internet Things J. 9 (23) (2022) 24541–24559.
[4] Yoann Dieudonné, Ducourthial Bertrand, Sidi Mohammed Senouci, COL: a data collection protocol for VANET, in: 2012 IEEE Intelligent Vehicles Symposium, IEEE, 2012, pp. 711–716.
[5] Raw, Shringar Ram, Manish Kumar, Nanhay Singh, Security challenges, issues and their solutions for VANET, Int. J. Netw. Secur. Appl. 5 (5) (2013) 95.
[6] Ali Hussein, Imad H. Elhajj, Chehab Ali, Ayman Kayssi, SDN VANETs in 5G: an architecture for resilient security services, in: 2017 Fourth International Conference on Software Defined Systems (SDS), IEEE, 2017, pp. 67–74.
[7] A. Bazzi, G. Cecchini, M. Menarini, B. Masini, A. Zanella, Survey and perspectives of vehicular wi-fi versus sidelink cellular-V2X in the 5G era, Future Internet 11 (2019) 122.
[8] Hidayet Aksu, Leonardo Babun, Mauro Conti, Gabriele Tolomei, A. SelcukUluagac, Advertising in the IoT era: vision and challenges, IEEE Commun. Mag. 56 (11) (2018) 138–144.
[9] E.M. El-Bakary, E.S. Hassan, O. Zahran, S.A. El-Dolil, F.E. Abd El-Samie, Efficient image transmission with multi-carrier CDMA, Wireless Pers. Commun. 69 (2013) 979–994.
[10] Alheeti Ali, M. Khattab, Gruebler Anna, McDonald-Maier Klaus, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks.", Computers 5 (3) (2016) 16.
[11] Mustafa Maad Hamdi, Lukman Audah, Sami Abduljabbar Rashid, Alaa Hamid Mohammed, Sameer Alani, Shamil Mustafa Ahmed, A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs), in: 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, 2020, pp. 1–7.
[12] Enrico Steiger, Bernd Resch, João Porto de Albuquerque, Zipf Alexander, Mining and correlating traffic events from human sensor observations with official transport data using self-organizing-maps, Transport. Res. C Emerg. Technol. 73 (2016) 91–104.
[13] Hammad Shafiq, Rana Asif Rehman, Byung-Seo Kim, Services and security threats in sdn based vanets: a survey, Wireless Commun. Mobile Comput. 2018 (2018).
[14] Brandon Craig Rhodes, James A. Mahaffey, James D. Cannady, Multiple self-organizing maps for intrusion detection, in: Proceedings of the 23rd National Information Systems Security Conference, MD Press, Baltimore, 2000, pp. 16–19.
[15] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, Mahdi Zareei, Mohammad Hossein Anisi, Cesar Vargas-Rosales, Muhammad Khurram Khan, ShidrokhGoudarzi, A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing, IEEE Access 5 (2017) 15619–15629.
[16] Sarah Oubabas, Joel JPC Rodrigues RachidaAoudjit, Talbi Said, Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme, Vehicular Communications 13 (2018) 128–138.
[17] Fotohi, Reza, YaserEbazadeh, Mohammad SeyyarGeshlag, A new approach for improvement security against DoS attacks in vehicular ad-hoc network, arXiv preprint arXiv:2002 (2020) 10333.
[18] Azhdari, Mohammad Sadegh, Barati Ali, Barati Hamid, A cluster-based routing method with authentication capability in Vehicular Ad hoc Networks (VANETs), J. Parallel Distr. Comput. 169 (2022) 1–23.
[19] Guandong Liu, Na Fan, Chase Q. Wu, Xiaomin Zou, On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks, Sensors 22 (14) (2022) 5361.
[20] Swapna Choudhary, Sanjay Dorle, A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc network s using machine learning-based blockchain routing, Concurrency Comput. Pract. Ex. (2022), e6993.