Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9642774, 13 pages
https://doi.org/10.1155/2022/9642774

Research Article

Transmit Range Adjustment Using Artificial Intelligence for Enhancement of Location Privacy and Data Security in Service Location Protocol of VANET

Shivkant Kaushik,[1] Ramesh Chandra Poonia,[2] Sunil Kumar Khatri,[3] Debabrata Samanta,[4] and Partha Chakraborty[5]

[1]*Amity Institute of Information Technology (AIIT), Amity University Jaipur, Rajasth An-303002, India*
[2]*Department of Computer Science, Christ University, Bengaluru, Karnataka 560029, India*
[3]*Amity University Tashkent, Uzbekistan*
[4]*RIT Kosovo (A.U.K), Rochester Institute of Technology – RIT Global, Dr. Shpetim Rrobaj, Germia Campus Prishtina 10000, Kosovo*
[5]*Department of Computer Science and Engineering, Comilla University, Cumilla-3506, Bangladesh*

Correspondence should be addressed to Partha Chakraborty; partha.chak@cou.ac.bd

Received 23 June 2022; Accepted 16 August 2022; Published 16 September 2022

Academic Editor: Kuruva Lakshmanna

IoT or the internet of things is the talk of the town topic being researched in the field of information technology for more than decade. It is being in deployment stage in various developing economics, to enable driverless automobiles in the field of VANET. It helps in preventing crashes and provides urgent medical assistance in emergency case. Data security and location privacy are becoming of most importance in present IT scenario. Unauthorized access to location information of vehicles may pose a significant security threat. So, it is necessary to secure the location information of the vehicle. The proposed work aims at enhancement of location privacy data security in service location protocol of VANET'S. The primary techniques to be employed include artificial intelligence-based RF range approximation for transmission range adjustment and receive RF strength based distance estimation for trusted node location perimeters approximation, dynamic adjustment of silence period of OBU (on based unit) in conjunction with radio/RF interrupt. The unauthorized access to location information of vehicles and need of its privacy is the motivation for this work.

1. Introduction

Intelligent transportation systems (ITS) are critical to make individuals' lives easier in every aspect of their daily lives in the digital age. The goal of ITS is to improve trac efficiency by reducing trac issues and limiting unwelcome occurrences [1, 2]. A wide range of services are provided by the ITS, including road safety, reduced congestion, and improved traffic flow on the road. As a result, automobile manufacturers have come to recognise that their cars must be connected to IT system; for example, intervehicle communication boosts safety and improves trac efficiency [3, 4]. In order to satisfy the needs and widen the recogniging event in cars, which cannot be done by using sensors, is accomplished. This technology allows cars in the immediate vicinity to monitor and exchange data on the flow of traffic, driver behaviour, and other aspects of driving. The introduction of vehicular ad hoc networks (VANETs) has made it possible to share information and boost the efficiency of communication in between cars. Today's automobiles are outfitted with a variety of high-tech features, such as GPS navigation, radar, and other on-board electronics (OBUs). To create a self-organized vehicular ad hoc network, wireless-enabled equipment make cars intelligent and capable of communicating with each other (VANET) [5, 6]. In order to facilitate wireless communication between cars, most suggested VANET system architectures call for automobiles to be equipped with a box that incorporates a radio

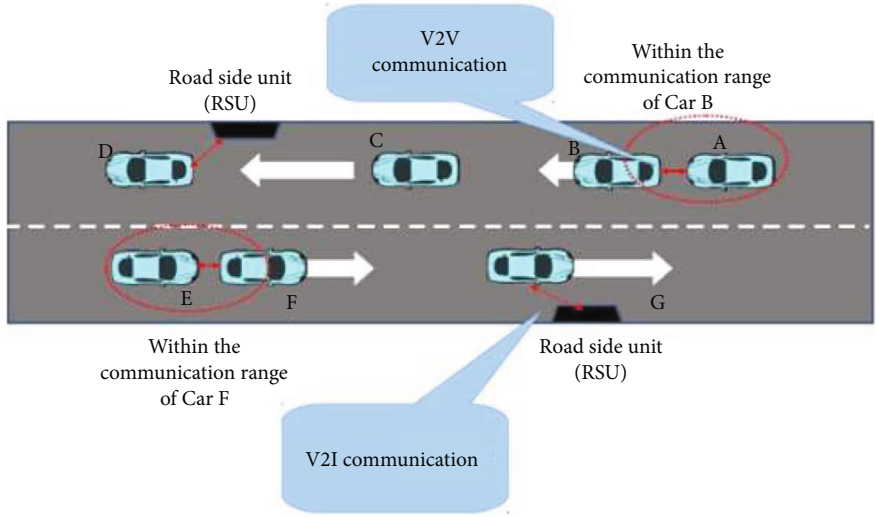

Figure 1: VANET vehicles communication system.

interface. VANET's quick mobility and changeable topology make it impossible to utilise the IEEE 802.11 wireless protocols in their current form, hence, IEEE designed a modified version of 802.11p for vehicle networks. The MAC layer was the most heavily modified. VANETs, on the other hand, have long been regarded as innovative and groundbreaking systems. Additionally, extensive study is conducted throughout the world before the actual technology is put into use in order to ensure the system's reliability and robustness [7–9]. It is a potential field for the development of ITS that aid drivers in increasing comfort and safety by providing beneficial services. V2V and V2I communication are the two basic kinds of VANET communication. Figure 1 shows VANET vehicles communication system.

In order to improve security and to provide variety of services to VANET users, vehicular mesh networks are being developed. The safety of service-oriented vehicle ad hoc networks is under threat from a variety of assaults. Service-oriented VANET security and privacy depend on the capacity to protect against many sorts of threats that exist in the VANET [10, 11]. It is the goal of this project to create internet-connected roadside infrastructures that can deliver a variety of data to VANET users. In this example, a car serves as a node in the VANET, which connects nodes for secure data transport. VANET is employed in the transportation industry to improve both safety and efficiency. Despite the fact that many traffic signals are employed to decrease road accidents, they are not very successful. VANET, on the other hand, employs a roadside unit. VAN users can get information from this RSU over the internet connection. Vehicles can communicate with one other and transmit alerts to each other to slow down or speed up, preventing accidents [12–14]. While travelling, internet access is available in every car. This roadside unit internet connection is faster than mobile internet, which is common nowadays. Due to the roadside unit's unique key, data sent between a car and RSU is more securely encrypted during transmission. This happens when a vehicle is pushed outside of the designated range. Old RSU's bending data will be moved to the new RSU. "Service-Oriented VANET" is the name given to roadside service. Different VANET security related issues are reviewed [1, 3, 4, 6, 7, 11, 13–15], and more secure systems are proposed then the previous [2, 5, 8–10, 12, 16–23] by different researchers.

2. Contributions to the Paper

(1) The proposed work of this paper is to the enhancement of location privacy data security in service location protocol of VANETS

(2) We train an artificial neural network for power estimation on required distance. We train network with some preselected data values, for the training of artificial neural network in our artificial neural network

(3) In this paper, we are showing that the proposed algorithm and artificial neural network will calculate Tx RF power required for required distance transmission

(4) Using a VANET service location protocol, the author has developed and shown a highly adaptable method for preserving location privacy and protecting data

Section 1 of the present paper explains about the introduction of VANET and different issues and limitations about it. Section 2 shows major contributions of this work. Section 3 discusses about the literature review of the related subject by different authors. Section 4 of this paper will talk about the methodology of the proposed system and proposed algorithm. The artificial neural network will calculate Tx RF power required for the required distance transmission. Section 5 will discuss about the results of proposed system along with performance analysis. Section 6 will discuss about the conclusion and the future scope of this article.

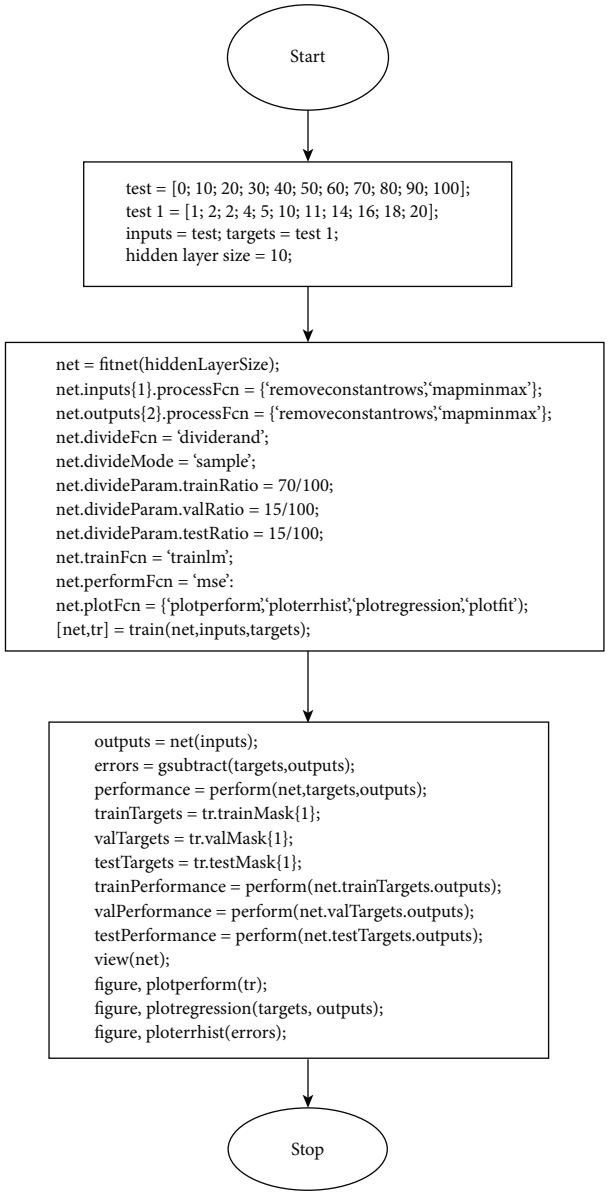

Figure 2: ANN flowchart.

3. Literature Review

According to Indu et al. [1], the VANET's primary concern is security. The security needs, assaults, and obstacles of implementing security measures in the VANET are covered in this study. The numerous VANET security methods put forth by various researchers are also examined and contrasted. When it comes to VANET, the most pressing concerns are security and privacy. The VANET, on the other hand, does not necessitate secrecy since most packets on the network do not include sensitive information. Considering that the majority of network assaults target the network layer, a safe routing protocol is essential to thwart these attacks.

According to Anju et al. [2], service-oriented VANET security and privacy provide a difficult challenge. Using an innovative and proven cryptographic technique, the proposed privacy-preserving data gathering and forwarding system overcomes these concerns. When compared to a more modern security mechanism, the suggested scheme's efficacy was shown to be superior. Clustering was also included as a factor in designing network and application systems. This study takes a look at a vehicle-based data sharing application [1]. A cluster of neighbouring vehicles is formed, with a few nodes chosen to serve as the cluster's leaders. These cluster heads act as local file servers, allowing other nodes in the network to upload and download files shared by the cluster. Clustering with multiple heads is proposed here. Unique to vehicular contexts, cars can either be travelling in the same way or in the opposite direction of each other. Experiments have shown that the clusters formed by the suggested approach have a long lifespan and are highly stable. There are plans for a multiheaded method, in which the single-headed algorithm is used to initially create clusters. In each cluster, there is a "master" CH (MCH) [2].

According to Mansour et al., as a result, VANET must solve a variety of security and privacy concerns in order to be broadly accepted by society. Because of this, researchers and businesses have been working to improve the security of communications in moving vehicles. In addition, new study topics in VANET include secure intervehicle communications with 5G-enabled automobiles and driverless vehicle security. VANET security and the privacy requirements were discussed in this study. It also provides a comprehensive breakdown of the many types of adversaries that may exist in the VANET. Additional information on the most prevalent VCS attacks and attackers has also been provided. Finally, our research shows that promoting VANET over the world necessitates the development of a safe privacy-preserving design [3].

According to Muhammad et al., because of its unique qualities, VANETs are seen as a more important and promising study topic in an intelligent transportation system, and as a result, security and privacy are major concerns. By broadcasting the safety alerts among cars and providing comfort services for passengers, VANET aims to protect human life on the roadway. The broadcasting of safety messages increases the vulnerability of VANET to assaults. This necessitates the development of a smart and resilient algorithm to combat serious security and privacy breaches [4].

According to Farouk et al., it was addressed in this work the location privacy issues that arise in VANET systems owing to unlawful monitoring of cars based on their broadcasts, and the possible user privacy threats related to identification of LBS apps are accessible from vehicles. The P2 FHE-AES method we suggested uses FHE over AES symmetric encryption to eliminate data noise and then outsources LBS data to the cloud while maintaining privacy [5]. AES-P2 FHE-AES enables the LBSP to conduct the query request while ensuring the confidentiality of VUis' inquiries and identification. It is also possible for the CSP to do computations on encrypted data in order to find the quickest route. As a result, RSUs, LBSP, and CSP are unable to access any information on our services [5].

According to Khan et al., hidden, asymmetric, and worldwide threats to data privacy are passive in nature.

Table 1: Description about the papers.

Year of publish	Author name	Title of paper	Brief description of paper
2015	Indu et al.	An analytic study of security solutions for VANET	The majority of network assaults target the network layer, a safe routing protocol is essential to thwart these attacks. Analytical study of security solution are discussed in this paper.
2015	Anju et al.	Secure data access through multiuser so-VANET	Service-oriented VANET security and privacy provide a difficult challenge. Using an innovative and proven cryptographic technique, the proposed privacy-preserving data gathering and forwarding system overcomes these concerns. Clustering was also included as a factor in designing network and application systems.
2018	Mansour et al.	VANET security and privacy—an overview	VANET security and privacy related issues are discussed along with the current state-of-the-art methods for meeting these needs. Most prevalent VCS attacks and attackers have also been discussed.
2019	Muhammad et al.	A comprehensive survey on VANET security services in traffic management system	In this paper, VANET security and privacy related issues are discussed for traffic management system. Safety alerts among cars provide comfort services for passengers and protect human life on the roadway.
2020	Farouk et al.	Efficient privacy-preserving scheme for location based services in VANET system	In this paper, for location privacy, P2 FHE-AES method is suggested that uses FHE over AES symmetric encryption to eliminate data noise and then outsources LBS data to the cloud while maintaining privacy.
2021	Khan et al.	Security challenges of location privacy in VANETs and state-of-the-art solutions: a survey	In this survey paper, various methods for protecting the privacy of roles in VANETs were laid forth. An introduction to VANET design and risk classes was provided by the authors.
2022	Gillani et al.	Data collection protocols for VANETs: a survey	Data collecting protocols for VANETs based on DTN, BE, and RT were discussed in detail in this article.
2020	Dukiya et al.	A location privacy framework using edge computing in VANET	In this paper, the authors combine cutting-edge technology with essential aspects like as authentication, anonymity, and the analysis of accessible digital evidence.
2014	Saranya et al.	Data confidentiality and users' location privacy in VANETs	Data confidentiality and location privacy is accessed by a new cryptographic function proposed by the authors that allows RSU and users to get desired security level to exchanged communications. They utilise a portion of current packet's data to create a new set of encryption keys for use in the following packet.
2012	Hu et al.	Efficient and multilevel privacy-preserving communication protocol for VANET	The improved ring signature-based system developed by the authors, which is focused at securing vehicular communications. It is multilevel conditional privacy-preserving scheme.
2018	Taleb et al.	VANET routing protocols and architectures: an overview	In this paper, the authors address demands and applications of VANETs, categories of VANET routing protocols and architectures, and primary benefits and drawbacks of the various types of network routing protocols.
2013	Konstantinos et al.	Effective implementation of location services for VANETs in hybrid network infrastructures	A homogeneous network and heterogeneous network that combines 802.11p with LTE are both proposed and evaluated in this study for centralised location service in a VANET urban scenario.
2016	Poornima et al.	Review of security in VANET	Various security vulnerabilities, assaults, possible remedies, current difficulties, and solutions are explored in this article for vehicle-to-vehicle communication in intelligent transportation systems.
2015			

Table 1: Continued.

Year of publish	Author name	Title of paper	Brief description of paper
	Soleymani et al.	Trust management in vehicular ad hoc network: a systematic review	Trust management is discussed in a systematic manner for VANET in this review paper. Authors discussed the influence of trustworthiness on the quality of applications and data.
2017	Kaushik et al.	Comparative study of various protocols of DDS	Keeping in mind the features of DDS protocols, the authors compared these protocols in this review article.
2018	Kaushik et al.	Evolutionary study of service location protocol	The SLP protocol is discussed from its initial stage to current stage and its different areas of recent research in VANET is discussed in this paper.
2019	Muhammad et al.	A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)	Security services with threats and assaults on these services are described, and most current methods for every security service are presented in this paper.
2020	Goyal et al.	Development of hybrid ad hoc on demand distance vector routing protocol in mobile ad hoc network	Hybrid AODV technique is proposed in this paper that will incorporate with the MFR (most forward within radius) and firefly algorithm for detecting shortest path.
2020	Goyal et al.	Design and implementation of modified local link repair multicast routing protocol for manets	A new protocol named modified local link repair (MLLR) multicasting routing protocol is proposed in this paper.
2021	Mahmood et al.	Security schemes based on conditional privacy-preserving vehicular ad hoc networks	Strengths and limitations of security schemes are discussed in this paper. Different schemes of security are also compared.
2021	Dwivedi et al.	Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET	A blockchain-based protocol is proposed in this paper. This novel decentralized architecture for VANET is without the cloud server.
2021	Kumar et al.	Black hole attack detection in vehicular ad hoc network using secure AODV routing algorithm	For detection of black hole, a secure AODV routing protocol is developed. RREQ and RREP packets are improved in these protocols. Cryptography function-based encryption and decryption is used for security.
2021	Tejasvi et al.	Framework for anomaly detection in VANETs	Based on deep neural network, an anomaly detection framework is developed for VANET using sequence reconstruction and thresholding algorithm.
2020	Bensaber et al.	Design and modeling an adaptive neuro-fuzzy inference system (ANFIS) for the prediction of a security index in VANET	To get a prediction model of security for VANET, the authors proposed an applied adaptive neuro-fuzzy inference system (ANFIS). The authors simulate the network, then obtain database of attacks occurred, then analyzed it statistically, and show results using MATLAB.
2019	Neelaveni et al.	Performance enhancement and security assistance for VANET using cloud computing	RSUs are replaced by cloud computing to enhance security during transmission of information, and the authors named this proposed work as modified vehicular-adhocNet
2016	Kirti et al.	VANET and its security aspects: a review	VANET security aspects are focused in this review article. The authors conceptually analyse these aspects.

VANETs, a type of modern cyber-physical equipment, are extremely profitable targets for the theft of personally identifiable information, thereby expanding the dangers and attack methods available. Physical assaults, such as mugging and stalking, may occur if a mobile VANETs node's location is violated. According to this study, the various methods for protecting the privacy of roles in VANETs were laid forth. An introduction to VANET design and risk classes was provided by the authors. This was followed by a discussion on location privacy and an examination of some of the most recent privacy-protection techniques. This solution's benefits have been studied extensively in academic literature. In addition to proposing several strategies to increase the security of VANETs, researchers have also worked to lower the amount of resources needed to implement these solutions [6].

According to Gillani et al., VANETs have come under fire recently because of their widespread use in ITS, the Internet of Vehicles (IoV), and smart city initiatives. In order to provide safe and seamless connectivity, data collecting has been extensively investigated in VANETs. The effectiveness, efficiency, timeliness, and cost-effectiveness of data gathering procedures are critical for ITS and IoV. Data collecting protocols for VANETs based on DTN, BE, and RT were discussed in detail in this article. To gain better understanding of categories and subcategories of VANET data gathering protocols, we used a hierarchical taxonomy design. A VANET's performance is dependent on several

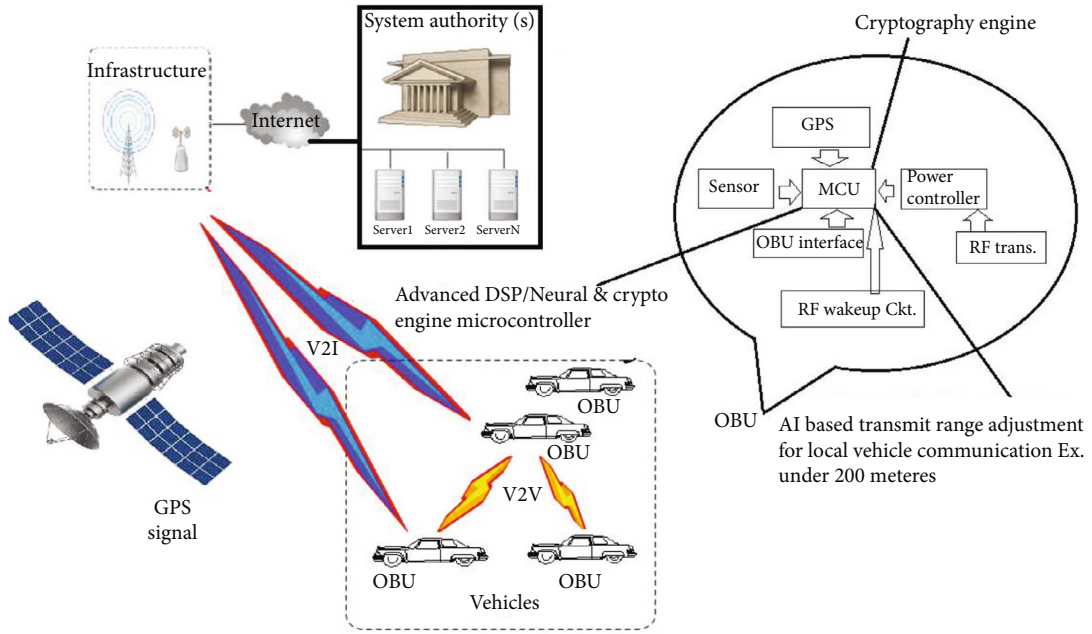

Figure 3: Proposed system architecture.

Table 2: Distance vs. power estimated.

S. no.	Distance in KM	Transmit power in Watts
1	10	2
2	20	9
3	30	4
4	40	5
5	50	8
6	60	11
7	70	14
8	80	10
9	90	9
10	100	20

factors, like packet drop ratio, packet delivery ratio, end-to-end delay, average forwarded messages, and recovery strategy; thus, each technique is extensively analyzed and evaluated [7].

According to Dukiya and Gajendra, in the vehicular networks, edge technologies are regarded to be the remodelling technology, since it alters the way gadgets and cars interact. By delivering characteristics like entire digital devices with sensing, computing, and communication capabilities, this technology has become a vital element of the vehicle networks and roadways. There are many exciting features that we may expect in the near future, such as extremely mobile, real-time apps that focus on security and privacy safety. In addition, being critical components of the analytical infrastructure for the intelligent transportation system, any attack on them may not only disrupt the network but also endanger human lives. This is the primary goal of this research project, which combines cutting-edge technology with essential aspects like as authentication, anonymity, and the analysis of accessible digital evidence [8].

According to Saranya et al., VANET is a subset of MANET, and it includes automobiles, trucks, buses, and motorbikes as nodes. Traffic and traffic restrictions, as well as the road course, limit the movement of nodes. The IEEE standard 802.11p for wireless communication is intended to be used by nodes communicating under the North American DSRC standard. Messages must be routed by other nodes in order to reach participants who are not within radio range (multihop communication). Users can register for a RSUs account using this secure web-based approach. During the registration process, users submit all of the necessary information so that they may benefit from safe connectivity from the moment they transmit their first packet to the RSU. The number of iterations of a new cryptographic function proposed by the authors allows RSU and users to apply the desired security level to exchanged communications. Authors utilise current packet's small portion data to create a new set of encryption keys for use in the following packet [9].

According to Hu et al., the improved ring signature-based system developed by the authors, which is focused at securing vehicular communications, is efficient multilevel conditional privacy-preserving [10]. Researchers show that their protocol not only provides the VANETs with the necessary conditional privacy but also increases vehicle economy by storing fewer keys per vehicle and allowing for the monitoring of a user's identification in the event of a disagreement. Our suggested method, on the other hand, is simple to implement, does not rely on roadside infrastructure or OBUs, and is completely safe against adversaries. As part of our ongoing research, we want to create a technique that maintains privacy by using ring signatures with constant-size signatures. Most ring signature-based

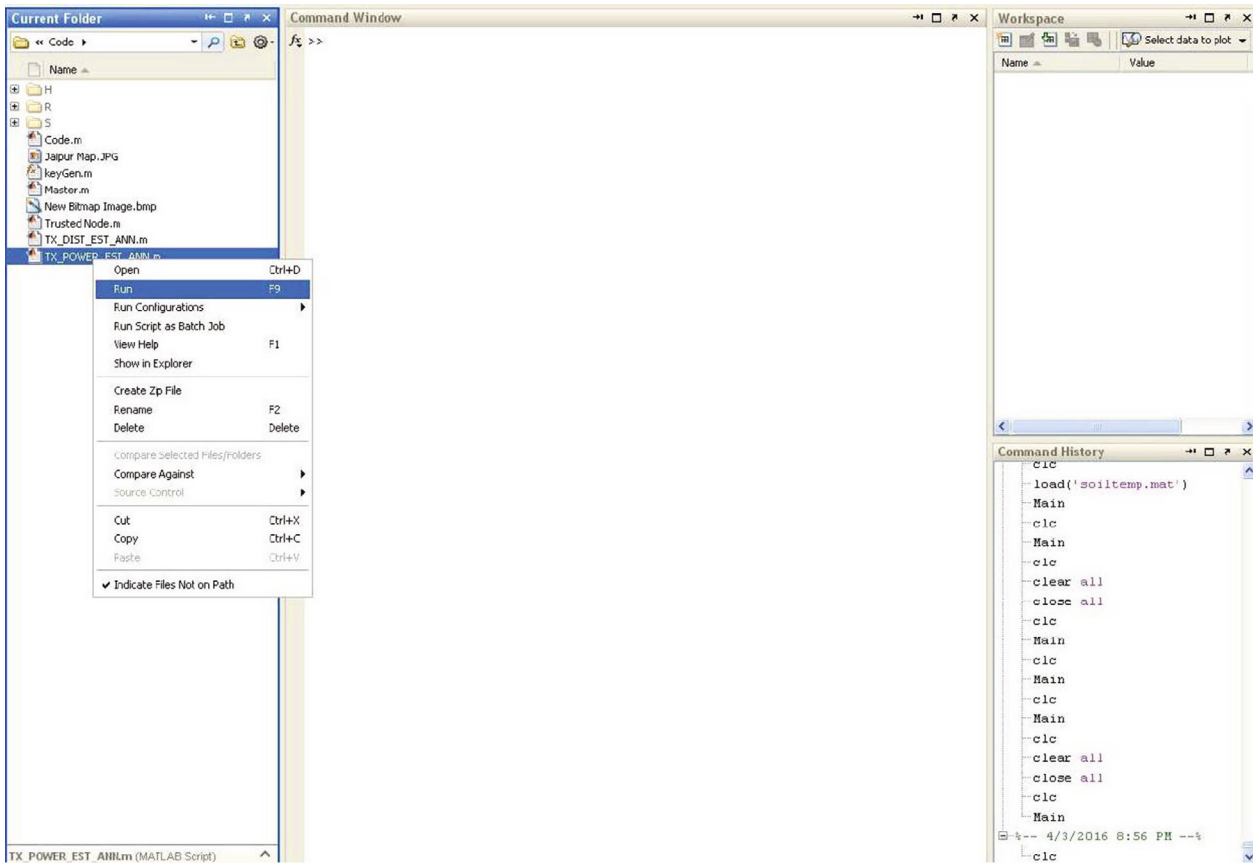

Figure 4: Run ANN code.

authentication schemes suffer from the fact that their communication cost is directly proportional to how many members they have. Many suggested ring signature techniques have signature lengths that is directly proportional to the rings number in the ring. Constant-size ring signature may be used to provide an efficient and secure authentication method for VANETs, according to the authors, this will be the focus of their investigation [10].

According to Taleb, because of the numerous ways in which VANETs might improve the safety of road travel, this is a rapidly growing field of study. It is mentioned here how VANET is distinct from its other subclasses of ad hoc networks. After that, the demands and applications of VANETs are discussed in detail. Other criteria for categorising VANET routing protocols are also addressed. VANET routing protocols and architectures are then described in the following sections. After that, we will go through the primary benefits and drawbacks of the various types of network routing protocols. Due to the enormous number of protocols, this document does not cover all routing protocols and applications of VANETs. For researchers who are interested in this field of study, we hope and aspire to offer fresh research possibilities and a launching pad [11].

According to Konstantinos et al., a homogeneous network 802.11p and a heterogeneous network that combines 802.11p with LTE are both proposed and evaluated in this study for centralised location service in VANET's urban scenario. The homogeneous networks function less well under high traffic and vehicle concentrations, according to the study's findings. Some traffic is offloaded from the 802.11p network by using the LTE network just for traffic relevant to LS, which reduces the LTE network's burden. Pure LTE networks might be an alternative for future ITS infotainment applications; however, a considerable number of sites (possibly femtocells) must be constructed, increasing infrastructure costs. Aside from ITS services, there are additional users on LTE networks that raise the network's background burden [12].

According to Poornima and Saboji, vehicle-to-vehicle communication (VANET) is an emerging technology. Intelligent transportation systems improve VANET efficiency (ITS). It has many of the same ad hoc network security problems. VANET makes attacks like eavesdropping, traffic analysis, denial of service, and reply attacks all too easy. Due to the unique nature of VANET, new security threats including unlawful tracking, position detection, and jamming are brought to the forefront. General cryptographic techniques in VANET include certificate systems for authentication and randomising traffic patterns, as well as symmetric session keys. Various security vulnerabilities and assaults are explored in this article, as well as possible remedies. Current difficulties and solutions are examined in this study [13].

According to Soleymani et al., using the trust model, vehicles can discern between trustworthy and untrustworthy

```
>> TX_POWER_EST_ANN

test =

     0
    10
    20
    30
    40
    50
    60
    70
    80
    90
   100


test1 =

     1
     2
     2
     4
     5
    10
    11
    14
    16
    18
    20
```

Figure 5: Test values used for ANN.

vehicles and communications. As a result, there is less chance of automobiles getting mislead by other vehicles. A comprehensive assessment is aimed at managing trust in VANET. There are several studies on trust models that have been reviewed in this article. The tools and measurements necessary to create and manage a trust model have been gleaned from this study, according to the authors. The authors have come to the conclusion that none of the trust models they have developed have met their goals in full. They then created a framework that includes probability, plausibility, trust assessment, and decision-making modules. This is why the authors came up with the framework. Fuzzy logic is used in these modules. Researchers can use this document to compile previously published work on trust models and identify new directions in which to pursue further research in this field. [14]

According to Kaushik et al., comparative study of different dynamic discovery service protocols (DDS) is done in the article on the basis of features of these protocols. DDS basic architecture is also discussed in brief by authors [24].

According to Kaushik et al., service location protocol (SLP) and its evolution are discussed by the authors in this paper. SLP and RFCs related information is also discussed. All the application areas of SLP where it is working now days is shown by the authors [25].

According Muhammad et al. [26], due to its high mobility and changeable network structure, the VANET is an interesting study field in ITS. For the purpose of ensuring the safety of pedestrians and drivers, it broadcasts safety warnings and offers passenger services. VANET is vulnerable to assaults since their safety announcements transmitted in open access setting. Security and privacy assaults can only be combated through the development of very effective algorithms. VANETs are the subject of this survey, which gives an in-depth look into the subject. We have already spoken about the VANET's basic model and operation. Finally, the security services with threats and assaults on these services are described. We have also explored in depth the authentication systems that guard the vehicular network from rogue nodes and bogus transmissions in great detail. As a third point of discussion, the authors looked at several simulation tools and how the authentication techniques performed in simulations. As a last step, we identified a number of VANET research difficulties and potential research objectives. For the most part, this review is comprehensive and incorporates the most recent developments in VANETs and security challenges, as well as privacy-preserving solutions [26]. According to Goyal et al., the hybrid AODV technique is proposed in this paper, and this technique will incorporate the MFR (most forward within radius) and firefly algorithm to detect shortest path [15]. In Figure 2, ANN flowchart, we can see the step by step executing of our ANN code. Table 1 shows description about the papers.

4. Methodology

This section will discuss about the methodology and concepts used in our work.

4.1. ANN Flowchart. ANN code is started in the first step; then, we call to test values in the next step; after that, in the next step, input and target test values will be provided; and then, hidden layer operation is performed in the next step. Then, we process some functions; then in the next step, some mathematical calculation will be performed; and then

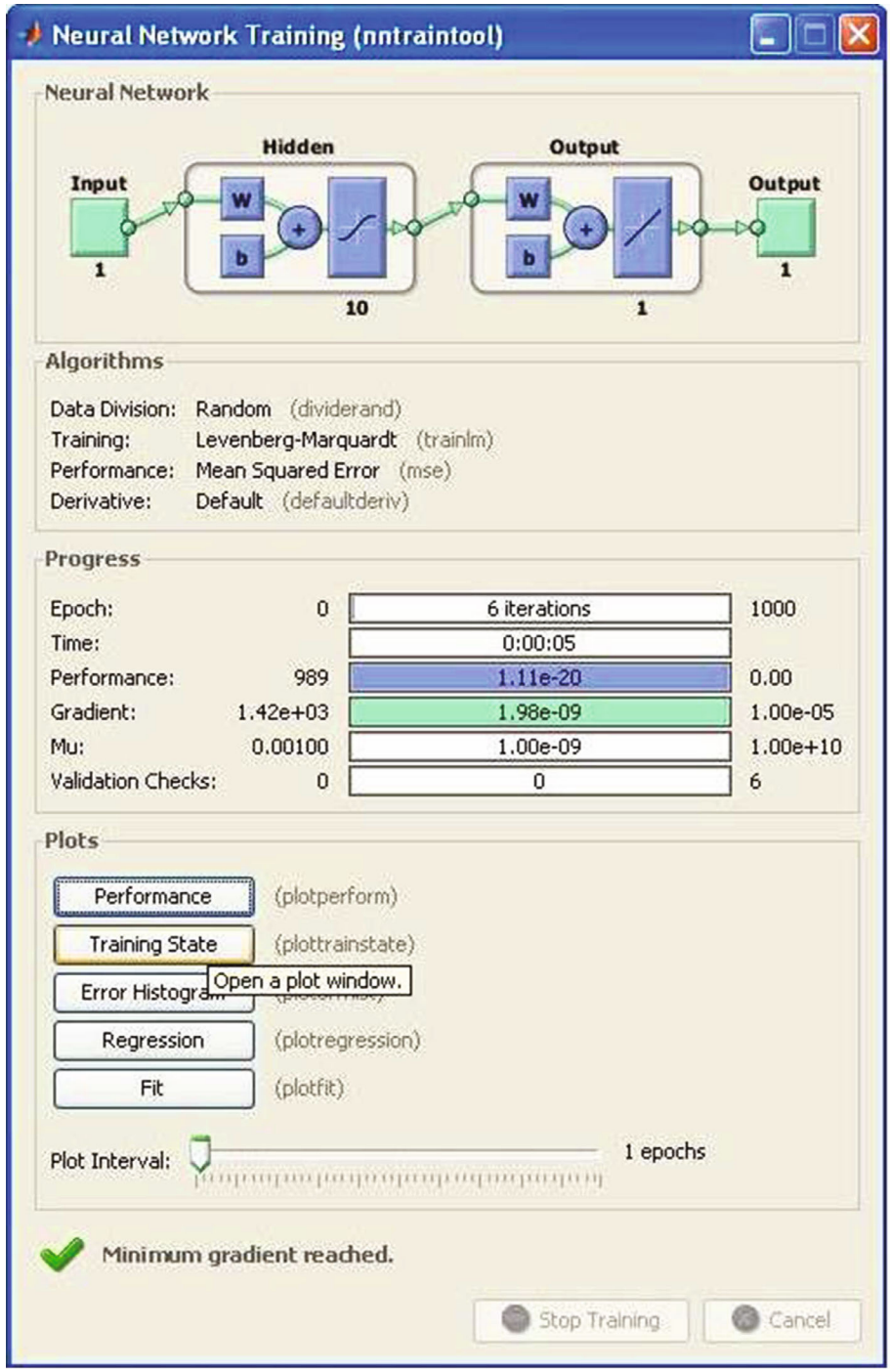

Figure 6: Neural network training.

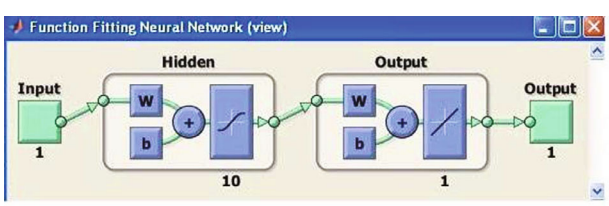

Figure 7: Function fitting neural network.

in the next step, train function will execute. Then in the next step, error graph and performance graph will be plotted to show the result. And in the last step, code will be stopped.

4.2. Proposed System Architecture. In the above Figure 3, proposed system architecture, we can see infrastructure connected to the internet and system authority also connected to internet. All the cars having GPS so these GPS are connected to satellite for finding own location. And we also

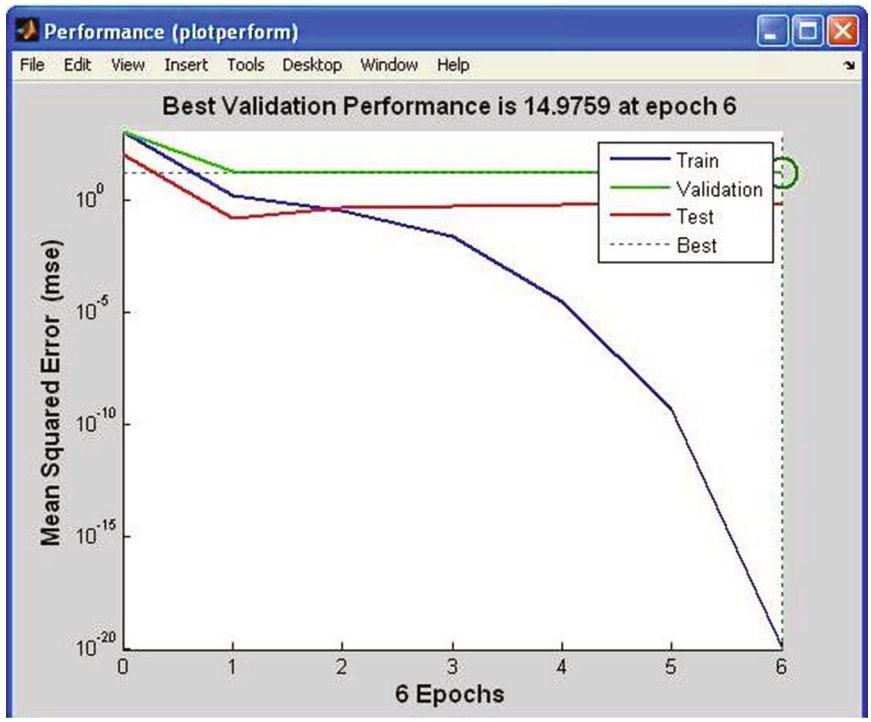

Figure 8: Best validation performance graph.

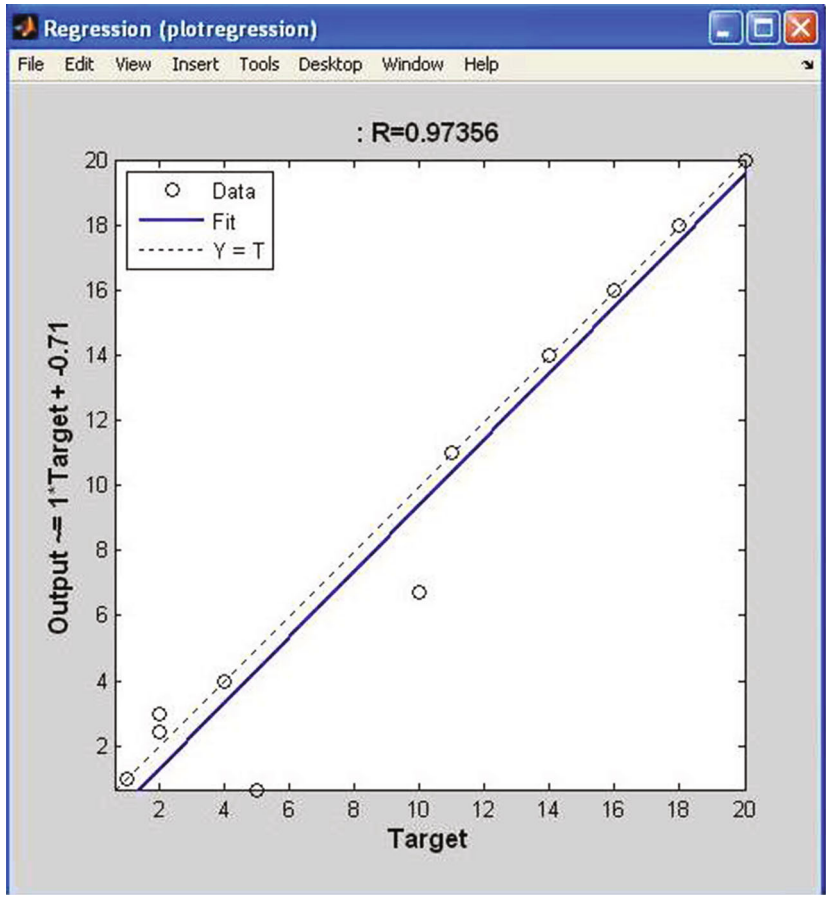

Figure 9: Regression plot.

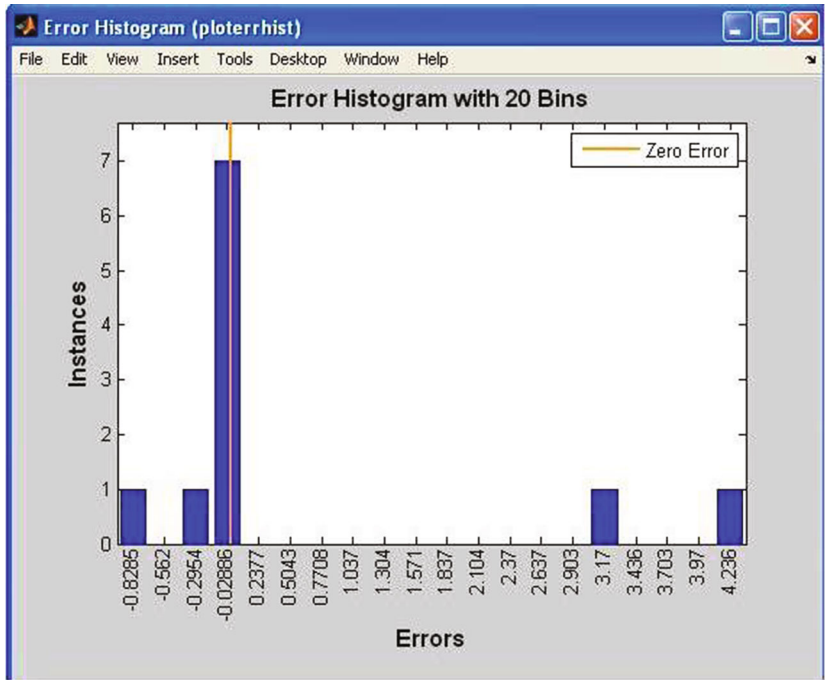

Figure 10: Error histogram.

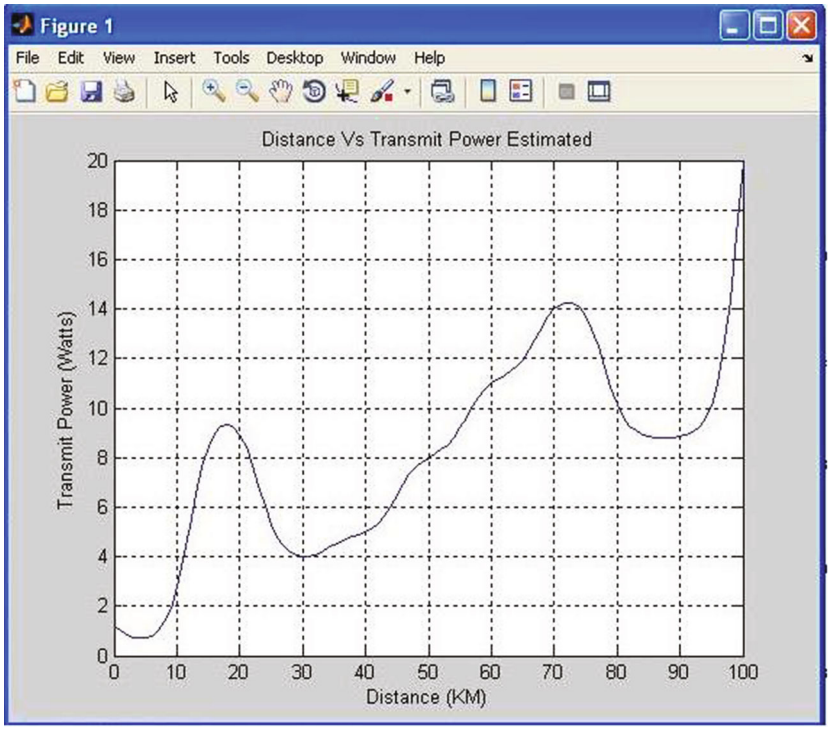

Figure 11: Distance vs. power estimated graph.

know that infrastructure coordinates with the network subscription that is stored in MCU. So now, we have our latitude and longitude related information and tower coordinated by using these data. Computer will calculate the distance and by using AI; we can transmit as required according to the distance calculated.

5. Results

In this paper, we are showing that here we train an artificial neural network for power estimation on required distance. We train network with some preselected data values, for the training of artificial neural network in our artificial

neural network we used 10 (ten) neurons with input and output, and here, we are plotting graph with required RF power estimate for transmission on required distance by our algorithm. These graph plots are showing in below results. So here, we are showing that our algorithm and artificial neural network calculated Tx RF power required for required distance transmission. In this section and subsection, we will show the step-by-step approach that we have used in our work to get the desired results. Table 2 shows distance vs. power estimated.

5.1. ANN Results. In this above Figure 4, we can see how we can run the ANN code by right click on the ANN code file then hit the run button. This is the procedure to run artificial neural network code file. In Figure 5, we can see the test values that are used for training artificial neural network. This is our training data set used for training ANN. In this above Figure 6, we can see neural network training part. Here, we use 10 neurons for training artificial neural network with input and output. And we can see that epoch is 6 iterations. In this above Figure 7, we can see function fitting neural network with input, output, and hidden part. In the above Figure 8, we can see best validation performance plot generated by our artificial neural network. Here, we can see train line, validation line, test line, and best graph line. In Figure 9, we can see regression plot between target and output values. In this above Figure 10, we can see error histogram plot generated by our artificial neural network.

5.2. Tx Power Estimation Results. Table 2 discusses the distance versus power estimated, and Figure 11 is its graph. In Figure 11, we can see graph between distance and transmit power. This graph plot is showing the main result of this paper. So here, we are showing that our algorithm and artificial neural network calculated Tx RF power required for the required distance transmission. In Figure 11, it shows that the RF range graph is not linear because of several factors such as a radio wave's power density drops when it travels a long distance, known as path loss. The weakening of the radio wave signals as they travel increases the likelihood of path loss. The power density of radio wave is proportional to the inverse square of the distance, and this is known as the inverse square law. Receiver sensitivity is the second most important component in determining range. There are two more factors that must be taken into consideration when making a calculation are fading margin and environment conditions. The height of the antenna can also have an impact on the available measurement range. The nonlinearity shown in the graph above is due to the nonlinear effects of numerous variables in the RF spectrum.

6. Conclusions and Future Scope

Using a VANET service location protocol, the author has developed and shown a highly adaptable method for preserving location privacy and protecting data. Artificial intelligence-based distance estimate algorithms for transmission range modification, received RF strength-based transmitter node distance approximation, and trusted node distance verification are used in combination to achieve this goal. A radio/RF interrupt is used in combination with an on-board unit's dynamic sleep/silence adjustment. Data privacy and security needs of the information age paradigm have been met with the development of a complete location privacy and data security improvement protocol for VANET.

(1) In future, apply this security scheme in V2V communication like cooperative driving to minimise traffic congestion and increase safety of vehicle

(2) Integration of biometrics for enhancement of data security node verification

(3) Radio frequency wave analysis/spectrum analysis to determine node RF signature word of malicious nodes

Data Availability

The evaluation data used to support the findings of this study are available on request from the corresponding author.

Disclosure

The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] B. Indu and K. Sibaram, "An analytic study of security solutions for VANET," *International Journal of Computer Applications*, vol. 132, no. 10, pp. 1–7, 2015.

[2] J. Anju and S. Deepu, "Secure data access through multiuser so-VANET," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, vol. 1, pp. 31–44, 2015.

[3] M. B. Mansour, S. Cherif, H. K. Mohamed, and S. A. Hammad, "VANET security and privacy - an overview," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 10, no. 2, pp. 13–34, 2018.

[4] M. S. Sheikh and L. Jun, "A comprehensive survey on VANET security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2423915, 23 pages, 2019.

[5] F. Fifi, A. Yasmin, and R. Rawya, "Efficient privacy-preserving scheme for location based services in VANET system," *IEEE Transactions*, vol. 8, pp. 60101–60116, 2020.

[6] K. Shawal, S. Ishita, A. Mazzamal, M. Z. Khan, and S. A. Khan, "Security challenges of location privacy in VANETs and state-of-the-art solutions: a survey," *Future Internet*, vol. 13, no. 4, pp. 1–22, 2021.

[7] G. Maryam, H. A. Niaz, M. U. Farooq, and U. Ata, *Data Collection Protocols for VANETs: A Survey*, vol. 8, no. 3, 2022, Springer, Complex & Intelligent Systems, 2022.

[8] D. Om and S. Gajendra, "A location privacy framework using edge computing in VANET," *International Journal of Applied Engineering Research*, vol. 15, no. 9, pp. 884–890, 2020.

[9] G. S. D. P. Nathiya and R. T. Amitha, "Data confidentiality and users' location privacy in VANETs," *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, no. 2, pp. 1391–1397, 2014.

[10] H. Xiong, C. Zhong, and L. Fagen, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Computers and Electrical Engineering*, vol. 38, no. 3, pp. 573–581, 2012.

[11] A. A. Taleb, "VANET routing protocols and architectures: an overview," *Journal of Computer Science*, vol. 14, no. 3, pp. 423–434, 2018.

[12] K. Konstantinos, D. Mehrdad, and L. Long, "Effective implementation of location services for VANETs in hybrid network infrastructures," in *2013 IEEE International Conference on Communications Workshops (ICC)*, pp. 521–525, Budapest, Hungary, June 2013.

[13] B. Poornima and S. V. Saboji, "Review of security in VANET," *International Journal of Engineering Research Technology (IJERT)*, vol. 4, no. 29, pp. 1–6, 2016.

[14] S. A. Soleymani, A. H. Abdullah, W. H. Hassan et al., "Trust management in vehicular ad hoc network: a systematic review," *Journal on Wireless Communications and Networking*, vol. 2015, no. 1, pp. 1–22, 2015.

[15] G. Ankur, V. K. Sharma, and K. Sandeep, "Development of hybrid ad hoc on demand distance vector routing protocol in mobile ad hoc network," *International Journal on Emerging Technologies*, vol. 11, no. 2, pp. 135–139, 2020.

[16] G. Ankur, "Design and implementation of modified local link repair multicast routing protocol for manets," *International Journal of Scientific and Technology Research*, vol. 9, no. 2, pp. 2316–2321, 2020.

[17] A.-s. Mahmood, A. Mohammed, A. Murtadha, M. Selvakumar, and H. Iznan, "Security schemes based on conditional privacy-preserving vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 479–488, 2021.

[18] S. K. Dwivedi, A. Ruhul, and V. Satyanaravana, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1913–1922, 2021.

[19] K. Ankit, V. Vijayakumar, K. Abhishek et al., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, p. 103352, 2021.

[20] A. Tejasvi, G. Bhavya, A. Ayush, C. Vinay, and R. Y. Fei, "DeepADV: a deep neural network framework for anomaly detection in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12013–12023, 2021.

[21] B. A. Bensaber, G. P. Caroly, and L. Youssef, "Design and modeling an adaptive neuro-fuzzy inference system (ANFIS) for the prediction of a security index in VANET," *Journal of Computational Science*, vol. 47, p. 101234, 2020.

[22] R. Neelaveni, "Performance enhancement and security assistance for VANET using cloud computing," *Journal of trends in Computer Science and Smart technology (TCSST)*, vol. 1, no. 1, pp. 36–45, 2019.

[23] Y. Kirti and P. Vijayakumar, "VANET and its security aspects: a review," *Indian Journal of Science and Technology*, vol. 9, no. 44, 2016.

[24] K. Shivkant, R. C. Poonia, and S. K. Khatri, "Comparative study of various protocols of DDS," *Journal of Statistics and Management Systems*, vol. 20, no. 4, pp. 647–658, 2017.

[25] K. Shivkant and C. Poonia Ramesh, "Evolutionary study of service location protocol," in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT 2018)*, pp. 159–164, Malaviya National Institute of Technology, Jaipur (India), March 2018.

[26] M. S. Sheikh, L. Jun, and W. Wensong, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.