Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2024.050819

ARTICLE

Privacy-Preserving and Lightweight V2I and V2V Authentication Protocol Using Blockchain Technology

Muhammad Imran Ghafoor[1], Awad Bin Naeem[2,*], Biswaranjan Senapati[3], Md. Sakiul Islam Sudman[4], Satyabrata Pradhan[5], Debabrata Das[6], Friban Almeida[6] and Hesham A. Sakr[7]

[1]Department of Engineering, Pakistan Television Corporation, Lahore, 54501, Pakistan

[2]Department of Computer Science, National College of Business Administration and Economics, Multan, 60000, Pakistan

[3]Department of Computer Science and Data Science, Parker Hannifin Corp, Chicago, IL 60503, USA

[4]Department of Electrical Engineering, University of Texas, Arlington, TX 76019, USA

[5]General Motors, Warren, MI 48092, USA

[6]Department of Computer Science and Data Science, ECOLABS, Aurora, IL 60503, USA

[7]Lecturer at Communications and Electronics Department, Nile Higher Institute for Engineering and Technology, Mansoura, 35111, Egypt

*Corresponding Author: Awad Bin Naeem. Email: Awadbinnaeem@gmail.com

Received: 19 February 2024 Accepted: 24 May 2024 Published: 31 October 2024

ABSTRACT

The confidentiality of pseudonymous authentication and secure data transmission is essential for the protection of information and mitigating risks posed by compromised vehicles. The Internet of Vehicles has meaningful applications, enabling connected and autonomous vehicles to interact with infrastructure, sensors, computing nodes, humans, and fellow vehicles. Vehicular hoc networks play an essential role in enhancing driving efficiency and safety by reducing traffic congestion while adhering to cryptographic security standards. This paper introduces a privacy-preserving Vehicle-to-Infrastructure authentication, utilizing encryption and the Moore curve. The proposed approach enables a vehicle to deduce the planned itinerary of Roadside Units (RSUs) before embarking on a journey. Crucially, the Certification Authority remains unaware of the specific route design, ensuring privacy. The method involves transforming all Roadside Units (RSUs) in a region into a vector, allowing for instant authentication of a vehicle's route using RSU information. Real-world performance evaluations affirm the effectiveness of the proposed model.

KEYWORDS

Vehicle-to-vehicle; vehicle-to-infrastructure; internet of things; block chain technology

1 Introduction

Integrating computer technology and the Internet of Things (IoT) has significantly transformed various aspects of daily life. Similarly, there is a paradigm shift in communication technologies, especially information security, such as front sensors, controllers, actuators, and other devices. These

technologies facilitate seamless transactions and information exchange between vehicles and their surroundings, improving decision-making and co-management [1]. Leveraging the capabilities of the Internet of Things in vehicles not only contributes to accident prevention but also encompasses features like intelligent automation, comprehensive data management, shared data utilization, intelligent navigation, and connectivity with mobile devices. The unique characteristics of IoT technologies necessitate their integrated functioning to optimize the future landscape of the Internet. This includes considerations for user experience, effective data management, and enhanced overall system performance [2]. Furthermore, the implementation of IoT services in the automotive sector, involving the integration of traffic, road, and environmental information, holds promise for reducing accident risks and enhancing security and overall performance.

However, the advent of IoT in vehicular applications raises concerns about data privacy and security. As vehicles become increasingly connected, drivers are required to submit sensitive information, such as vehicle details, location, and speed. The potential for data breaches and privacy infringements poses challenges that must be addressed to ensure user safety [3]. From an economic perspective, a cost-benefit analysis of blockchain and smart transport for governments and corporations becomes imperative. Key factors include course correction, administrative efficiency, housing optimization, and capital expenditure. Blockchain technology, with its focus on transparency and trust, offers a pathway to low-cost corporate environments, mitigating business instability through smart contracts and advanced data management techniques. Blockchain serves as a shared repository for digital, cryptographic, internet, and software-related information. Its attributes, such as registration, monitoring, openness, and disclosure, play a crucial role in preventing misuse and reinforcing system support [4]. The integration of blockchain with IoT enables real-time data integration and transfers, reducing processing time and fostering secure and reliable agreements [5]. In the context of Internet traffic protection, ensuring the integrity of vehicle and device data becomes paramount. Privacy is safeguarded through mechanisms that provide anonymity for users. Consequently, the automotive sector must prioritize the implementation of robust safety measures to protect users and their data [6]. The burgeoning growth of automotive applications and services, coupled with an increasing number of smart vehicles, poses challenges related to data and network traffic. The Internet of Vehicles (IoV), characterized by high mobility, low latency, contextual complexity, and heterogeneity, presents challenges for traditional cloud-based storage and management systems [7]. To address interoperability issues among IoV entities controlled by different service providers, a decentralized, distributed, interoperable, and scalable infrastructure is imperative. Blockchain technology, modern cryptography, and edge computing emerge as pivotal components to ensure the secure, private, and trustworthy transmission and storage of IoV data [8]. The contribution of the paper is that:

- To propose an advanced strong blockchain-based authentication in intelligent transport system (ITS).
- To implement the model based on objective.
- Evaluate the efficacy of blockchain-based authentication in Intelligent Transport Systems.
- Assess the impact of blockchain authentication compared to Pseudonym-based authentication.
- To determine the most straightforward and authentic Intelligent Transport System for transportation.

2 Literature Review

To slow down greenhouse gas emissions and fight climate change, the transportation sector is changing quickly. Countries like China and Saudi Arabia want to have 30% of their automobiles be

electric by 2030, demonstrating the growing popularity of electric vehicles (EVs) [7]. Research has been done to increase vehicle access control network (VANET) system efficiency and driving safety. Public key infrastructure (PKI), group signature, and identity-based schemes are the three primary types of VANET systems. Nevertheless, these systems encounter difficulties in storage and certificate administration, fast changes in VANET architecture, and high-speed vehicle movement [8]. For VANET systems, ID-based authentication approaches have been suggested as a solution to these problems. These techniques create private keys using a private key generator (PKG) and employ a pseudo-identity as the public key. These systems, however, are susceptible to batch verification issues, insider assaults, and system key escrow. Novel edge computing ideas, secure hash function-based and group-key agreement techniques, and VANET pseudonym-based authentication schemes with cuckoo filters have all been presented in recent attention-grabbing research; but, their safety, efficiency, and computational cost are all at risk. To solve crucial driving area and system key escrow issues, this study provides a lightweight pseudo-identity-based CPPA VANET solution that improves computation cost and communications overhead for the whole VANET system [9]. The system also resolves batch verification issues and TA bottlenecking and stops attackers or trustworthy cars from delivering harmful or phony beacons. The rapid advancement of information and communication technologies (ICT) has resulted in the creation of smart cities, necessitating effective traffic control and vehicle management. Mobile Ad Hoc Networks, or VANETs, are being developed to enhance weather forecasts, driving safety, passenger comfort, road conditions, and traffic congestion. Nonetheless, it is essential to guarantee security and privacy in VANETs as automobiles often transmit vital data, such as emergency alerts, which might be hacked by enemies. Prior research has tackled security concerns without emphasizing efficiency, resulting in unnecessary computational and communication overheads [10]. Research, education, and the automotive industry have all seen revolutionary changes because of the Internet of Vehicles (IoV). Ensuring appropriate authentication and secure communication is still a significant problem, however. This work uses cryptographic procedures to offer a lightweight mutual authentication mechanism for Internet of Vehicles (IoV) scenarios. To minimize computational expenses, the protocol allows a device and server to create a secret key for safe communication. Two Raspberry Pis linked via the cloud (Vehicle Server) and two Raspberry Pis connected via an intermediary desktop computer serving as the Trusted Authority (TA) are the two communication modes used to implement the protocol [11]. The suggested protocol outperforms current systems, according to the performance analysis findings. By examining mutual communications, trust models are added as a security feature to VANETs to identify insider threats. Trust models make sure that trustworthy data is disseminated across the network, that malicious cars are located, and that misleading messages are removed. Using blockchain technology in Vehicle Ad Hoc Networks (VANETs) may help build a strong trust model. It is a distributed ledger that keeps account of all digital events that are finished and shared between involved nodes, offering accurate and traceable information. Blockchain technology is a good fit for safe storage in VANETs because of its decentralization, transparency, immutability, and anonymity. Current authentication systems, including public-key infrastructure (PKI), have drawbacks such as long certificates and no privacy protection [12]. This research proposes a hybrid cryptography-based decentralized and scalable privacy-preserving authentication (DSPA) strategy for safe vehicular ad hoc networks. Compared to current authentication techniques, DSPA is more effective, decentralized, scalable, and privacy-preserving. Restricted mobility regions, fast network architecture, frequent network access, and security risks are some of the obstacles that VANET communication must overcome. Several authentication approaches have been put out to increase VANET efficiency and security [13]. To authenticate and transmit data in the VANET environment, cars use pseudonyms. This enables traffic authorities (TA) to trace and revoke rogue vehicles. Nevertheless, there are drawbacks to this strategy, including expense and inefficiency. The Chinese remainder theorem, the elliptic

curve discrete logarithm hypothesis, broadcast message authentication, identity-based cryptography, identity-based batch verification, group signatures, message authentication, and fully aggregated conditional privacy-preserving certificate aggregate signature are some other suggested schemes. These programs seek to protect privacy and security while enhancing traffic efficiency and road safety [14]. Fast-moving vehicles, or VANETs, are being employed more and more for commercial, traffic control, and commuter safety applications. Nevertheless, these networks are susceptible to security threats such as message repudiation, vehicle impersonation, and message manipulation. Many methods, including quantum cryptography, public-key cryptography, and symmetric-key cryptography (SKC), have been suggested to secure these networks. These approaches, however, depend on computationally challenging issues and are slower. Because of the Heisenberg Uncertainty Principle and the no-cloning theorem, quantum cryptography—which combines quantum operations with conventional cryptography—offers absolute security. This work proposes a new privacy-preserving authentication technique for VANETs since, despite these advances, the current methods do not offer vehicle identity privacy [15]. Because they are open wireless networks, vehicular ad hoc networks, or VANETs, are susceptible to security assaults. To tackle this issue, a protocol and architecture for conditional privacy-preserving authentication with dual blockchain assistance is suggested for VANETs. This system eliminates the need for a centralized, trustworthy third party and enables identity authentication and privacy protection [16]. Additionally, conditional monitoring of unlawful cars and decentralized dynamic revocation of illegal vehicles via smart contracts are made possible by the proposed approach. By extending the traditional blockchain structure, the Merkle Patricia Tree (MPT) data structure offers a distributed authentication method that does not need a revocation list [17]. By including trust assessment and taking into account vehicle behavior variables, the proposed dual authentication approach for the Internet of Vehicles (IoV) tackles security and privacy problems. A blockchain and elliptic curve cryptography (ECC)-based efficient cross-datacenter authentication and key-exchange strategy is presented, resulting in improved security characteristics with lower computational and communication overheads [18]. To provide safe and effective data transmission across a public channel for vehicle ad hoc networks (VANETs), the paper provides a simple, privacy-preserving authentication system. Compared to state-of-the-art protocols, the protocol is less computationally and communication intensive, safe, and scalable. The protocol uses a three-layered infrastructure design and physical unclonable features to overcome security challenges in the Internet of Vehicles (IoV) [19]. The suggested approach shows resilience against several kinds of attacks and drastically lowers the number of authentication packets and MAC/PHY overhead. To enhance living in smarter cities, the study also addresses the proliferation of smart gadgets and the Internet of Things. Roadside Units (RSUs), trusted authorities (TAs), cars, and a traffic management and control center (TMC) make up a vehicle-aided network, or VANET [20]. Every vehicle is equipped with an on-board unit (OBU) for inter-node communication. Whereas the TAs provide secure services, the RSUs deal with traffic-related services [21]. Traffic data is gathered and examined by the TMC from RSUs. Vehicle-to-vehicle and vehicle-to-infrastructure communication is used. Due to the high mobility and quantity of vehicles, conventional cloud computing is inefficient [22]. Cloud computing's counterpart, fog computing, may move cloud services and apps to the network's edge, resolving these problems. To guarantee a safe and effective VANET architecture, issues with identification, privacy, and location must be addressed. scholars have investigated many methodologies to tackle privacy and security issues in Vehicle Ad Hoc Networks (VANETs). Numerous authentication methods, such as identity-based, group signature-based, certificate-based, and pseudonym-based systems, have been created [23]. These methods still have problems with efficiency, security, and privacy. Researchers are creating certificate authentication schemes—which only offer a partial private key and do not need a certificate—to overcome these issues. Created for Bitcoin applications, blockchain technology offers a potential way to bring trust

and transparency to VANETs [24]. Pseudo-anonymity, privacy, secrecy, and fairness are all achieved with it. To accomplish Vehicle to Infrastructure (V2I) authentication, V2I handover authentication, and Vehicle to Vehicle (V2V) broadcasting authentication, a blockchain-based protocol is suggested. With the help of dynamic anonymity techniques, vehicle feature embedding strategies, lightweight V2I handover authentication, and Physically Unclonable Functions (PUF) technology, the protocol can withstand captured attacks and broadcast verifiably without the need for transportation infrastructure or Trusted Authorities [25].

3 Proposed Methodology

We classify the protocols used in VANETs to protect privacy, authenticate users, and distribute secure messages into several categories and examine the advantages and disadvantages of each protocol within each category. Because several protocols might be classified in more than one category, it's impossible to give a definitive classification of them all. This is merely a generalization.

3.1 Network Model

There are three key players in the VANET system model: an Authentication Server (AS), a large number of Roadside Units (RSUs), and a large number of cars. The AS is presumed to be completely trustworthy, while RSUs are thought to be just somewhat trustworthy, and cars are presumed to be completely untrustworthy. As a result, each vehicle is expected to contain an on-board unit (OBU) with limited processing and storage capabilities that communicate with the RSUs. The on-board unit (OBU) will be used to designate a specific vehicle in the following sections. Furthermore, with VANET, neither the wired nor the wireless channels are expected to be secure. A hacker can therefore intercept messages being delivered and use them to conduct various attacks.

3.2 System Model

Fig. 1 depicts a simple model made up of three components: a CA, an RSU, and a vehicle.

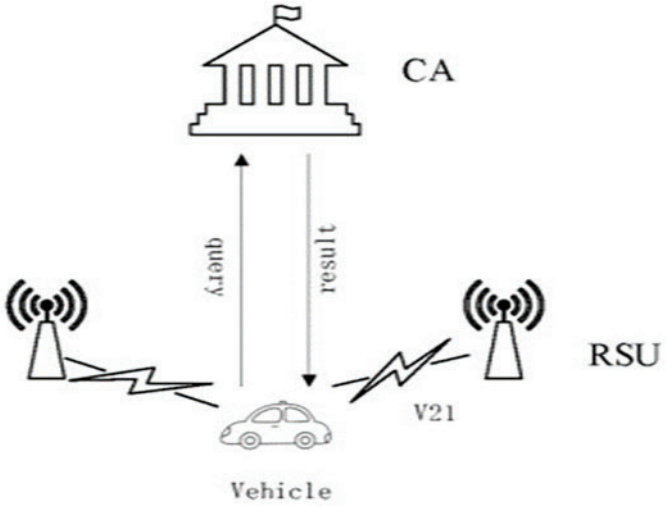

Figure 1: System model

A semi-trusted certificate authority (CA) may try to derive valuable information from legally received messages. In addition, CA manages VANETs and helps RSU verify the vehicle by storing

RSU information. It receives and passes on the information from a vehicle within its range via RSU. OBU and TPD modules installed in a vehicle communicate information with RSU and CA, while TPD keeps private data for secure computing.

3.3 Design Goals for ITS

Message Integrity: One of the most important considerations in the design process is message integrity, which means that any changes made to an open channel message should be detected by the receiver. Message confidentiality: The eavesdropped message is useless to an attacker.

3.4 Rout Plan Privacy

If all RSUs are compromised, the genuine identification of the vehicle cannot be deduced because the RSU and CA cannot collaborate. Ride-sharing anonymity: CA assists a vehicle in obtaining RSUs' information on its route, but does not know which RSUs' information has been gleaned. A new ITS design is proposed that incorporates blockchain technology. Overlays of hierarchical blockchain are built on top of the vehicular network infrastructure in this architecture. Because no new network entities are added, the ITS's existing services can be used with confidence. Protecting user privacy, while reducing the likelihood of a system or service failing due to a single point of failure is made possible by the blockchain's decentralization and anonymity. Because of the immutability of the blockchain, data integrity and evidence of hostile activity in the intelligent transportation systems are both guaranteed. New intelligent transportation system services can be launched quickly and easily using blockchain's smart contracts. Meanwhile, legacy vehicle networks can continue to analyze and transmit data efficiently. Ultimately, we want to encourage vehicles and ITS users to actively participate in the intelligent transportation system by providing and utilizing data. The following are the primary contributions. Blockchain technology can be integrated into the current intelligent transportation system design and procedures. Users' privacy is protected by the planned blockchain-aided transportation system (Ba-ITS), but the system is also backward compatible with the old intelligent transportation system, making it a viable option for the transportation industry. To propose a hierarchical blockchain framework, allowing for the system's scalability. Consideration is given to the interoperability of different blockchain layers as shown in Fig. 2. Extensive examples of how smart contracts and blockchain-related messaging might be coupled to create efficient new services will be presented. The Intelligent Transport System oriented Blockchain Model with seven layers is proposed in the figure below.

3.5 Privacy-Preserving Lightweight Architecture

PLV scheme has four stages: initialization, registration, query, and authentication. CA produces and publishes security parameters, as well as RSU information, during the first phase. This information is exchanged when registering with the California Automobile Association (CA). The vehicle queries CA during the query phase and deduces the information of RSUs along its route; nevertheless, CA is unaware of which RSUs' information has been deduced by the vehicle during this phase. After that, vehicle and RSU rapid authentication is achieved.

3.6 Vehicle to Vehicle and Vehicle to Infrastructure Communications

V2V communications are used between vehicles, while V2I communications are used between vehicles and the roadside infrastructure. Designing a VANET while considering vehicular mobility is a difficult task, this project gives you a fundamental understanding of how vehicular mobility

affects the density of VANET networks and the connectivity between V2V and V2I. Valet mobility is required for VANET designers in the future. Examples of this mobility include connectivity under specific road traffic situations inside specific geographic locations; routing protocols for multi-hop-based applications; or security and privacy threats and mitigations. To test connectivity and network performance, you'll need tools that make building and visualizing VANET scenarios easy. As a result of working on this project, you will have improved design skills. Section one and section two of this project are separate. In the first phase, you will simulate highway mobility to evaluate the network densities available for V2V connectivity under various traffic volumes. In the second half, we'll practice using a graphical tool to visualize and evaluate two different VANET situations that you specify. A vehicle-to-vehicle (V2V) communication; a vehicle-to-remote sensing unit (RSU) V2I communication.

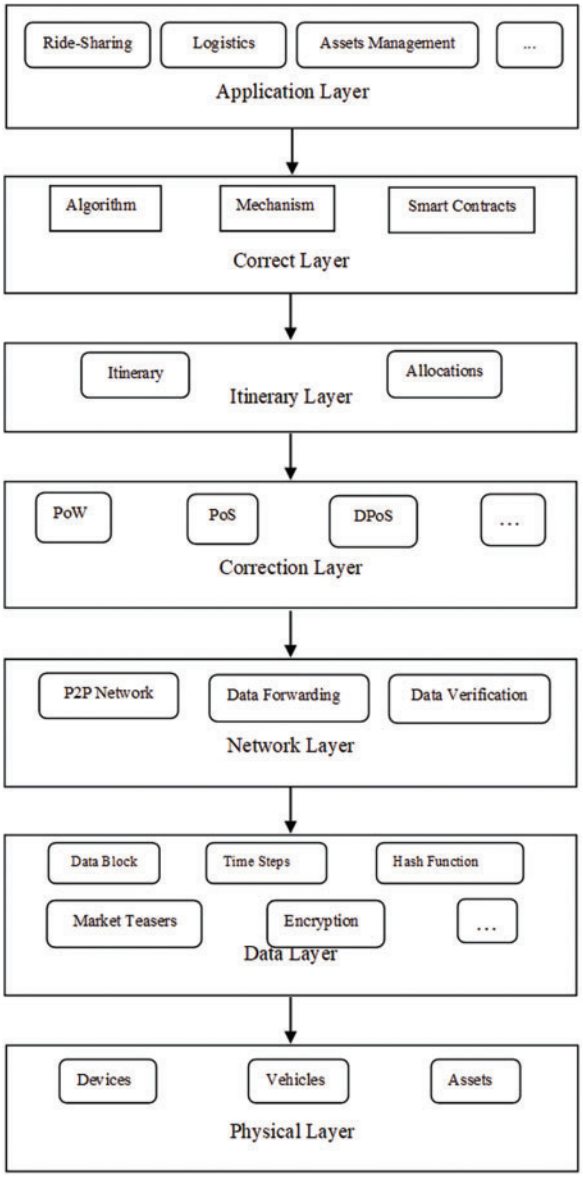

Figure 2: Intelligent transportation system oriented blockchain framework

3.7 Blockchain-Based Service Sharing via Road Side Units

Vehicles in this model have already been registered by the revocation authority in this model. In addition, BC includes vehicle data and a timestamped record of prior car-sharing services. RSU assists vehicles in requesting services from other vehicles on their needs. Whenever a vehicle sends out a request, the RSU receives it. Response vehicles' services have already been entered into RSU's database. This request will be sent to the network by RSU. Messages will be sent out to every car connected to the network. After that, the available car will contact the one that was requested. Smart contracts will be generated between the responding and responding cars if both vehicles agree to the terms of the smart contract when they agree to share their services. To mine the blocks, POW is needed, and it is also included in each transaction. Consensus mechanisms were then utilized to verify the block's validity and add it to the BC. Fig. 3 shows the proposed model of blockchain services sharing in ITS.

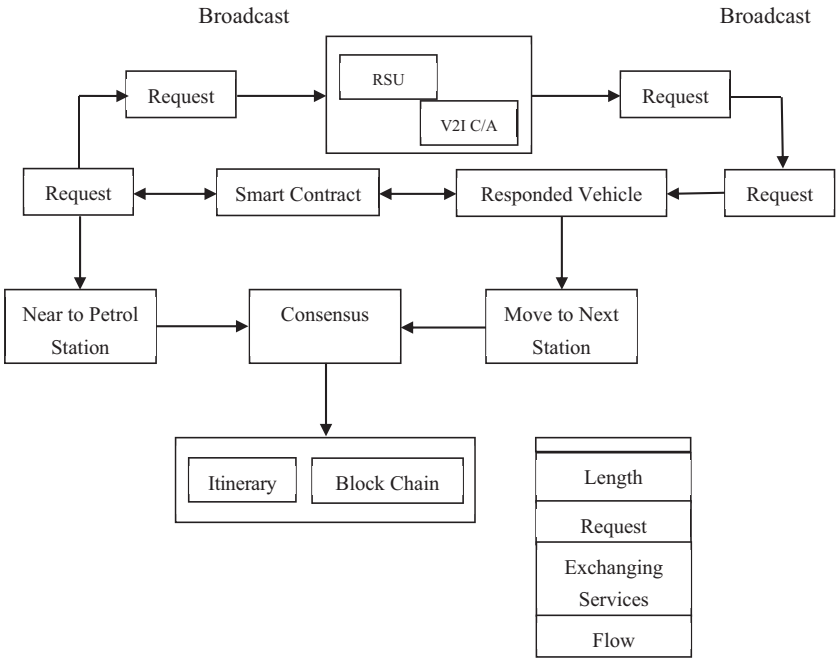

Figure 3: Proposed model of block chain services sharing in ITS

4 Results and Discussion

In this section, our proposed system is scrutinized to ensure message integrity; message confidentiality, vehicle anonymity, and route plan secrecy are all met. Authentication, TPD pre-computation, and CA computation all play a role in determining performance.

In Fig. 4, we examine the following communications:

- Vehicle-to-vehicle communication between vehicles and RSUs
- The time delay with several cars

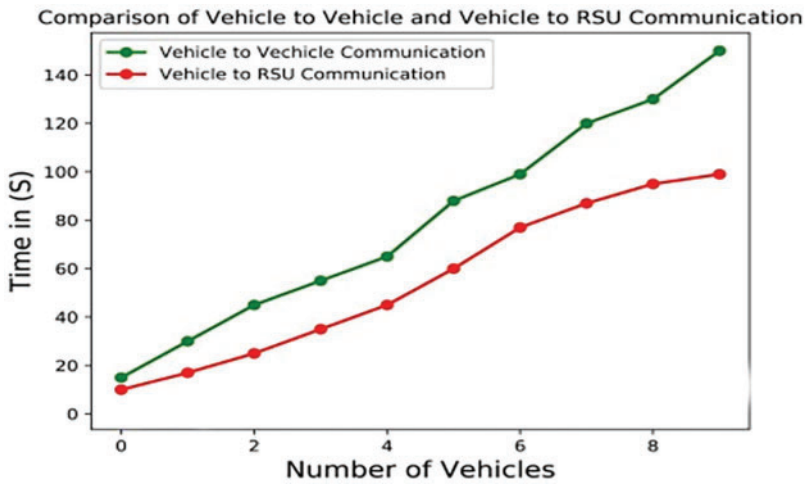

Figure 4: Comparisons between vehicle to vehicle and vehicle to RSU

It takes longer for vehicles to communicate with each other than it does for vehicles to communicate with RSUs. Slowly, the amount of time it takes to complete a task grows. Vehicle-to-vehicle communication has a lower throughput than RSU. This shows that the delay rate in both communication channels is growing. However, the delay from a vehicle to an RSU is minimal.

In Fig. 5, the *x*-axis shows the number of blocks, while the *y*-axis shows the cost. As the number of blocks increases, so does the operational expense. Operating costs rise when contracts are signed. On the other side, when a smart contract function is called, operational costs are reduced.

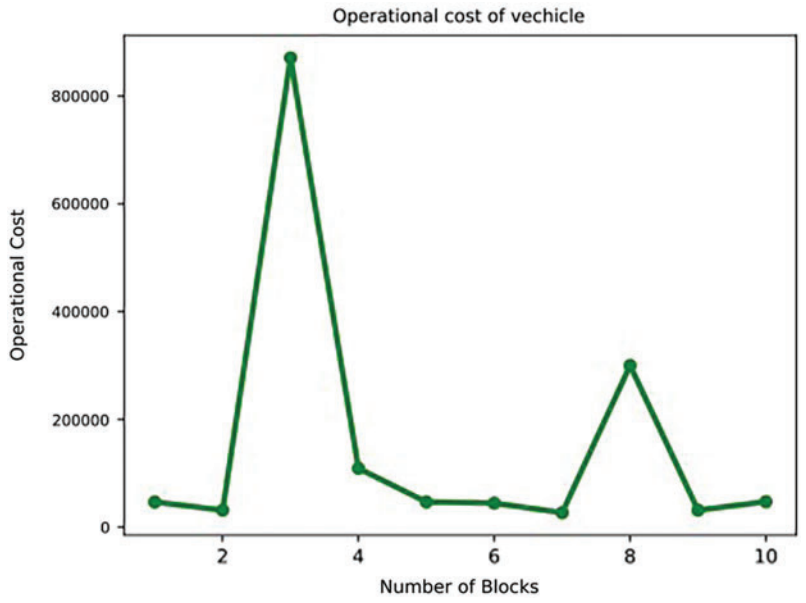

Figure 5: Operational cost

Another thing that's needed to capture how a car moves behind another car on the road or how a car changes lanes to pass the car ahead of it is behavior models for cars following and changing lanes

[2] and [3]. The model of freeway transportation describes that each vehicle is spatially constrained to a single lane of the freeway, and its speed is time-dependent on its previous velocity. In the same way, if two vehicles are traveling in the same lane within a safety distance (Ds), then a car following it is spatially dependent on the car ahead of it, which we'll call the leading vehicle. As a result, for vehicle I the intra-vehicle relationship is:

New speed = current speed + random () * acceleration

where **random** returns a value uniformly distributed in [−1, 1] and equally probable vehicle deceleration or acceleration. Additionally, if vehicle j is ahead of vehicle I in its lane and inters vehicle distance Ds, then speed I speed j is the resulting inter-vehicle relationship.

4.1 Simulation Parameters

The above models must be put into action under the simulation conditions outlined in the following section. These simulation conditions are summarized in Table 1.

Table 1: Simulation parameters

Parameters	Value
Safety distance (Ds)	10 m
Vehicle speed S min	50 miles/hour = 22.35 meters/seconds, S max = 70
Miles/hour	31.29 meters/seconds
Vehicle acceleration	a_min = 0 meters/seconds^2, a_max = +(−)5 meters/seconds^2
Road traffic volume	Vol = 3000 vehicles/hour/lane
Vehicle arrival rate/Departure rate	0.833
Road traffic density	100–500 vehicles/lane
Minutes	2
Range	50

The simulated freeway map is shown in Fig. 6 below. Each lane on the motorway must be 5000 m long, and there must be three entry ramps and three exit ramps that are used by vehicles on all four lanes. Fig. 6 shows a simulated four-lane, five-kilometer motorway with a three-meter inter-lane separation and a one-direction separation. The average number of vehicles per motorway lane might range from [100, to 500] depending on the freeway's density of vehicular traffic. In addition, cars' starting speeds and acceleration must be distributed uniformly. It's assumed that freeway traffic flow is 3000 vehicles/hours per lane, thus the inter-arrival and inter-departure process for each lane is kept exponential at 3000/(6060) = 0.833. To be clear, we're using actual traffic density and volume statistics. Note: In MATLAB, you may use the expressions rand arrival rate and rand departure rate to calculate the arrival and departure rates of new vehicles and current nodes per lane using an exponential distribution. In AVISPA simulation, these expressions produce a random value of 0 or 1, depending on how they are applied. An entry ramp is chosen by chance only if there is no existing node on the highway; otherwise, it is chosen by chance only if there is an existing node on the motorway and an exit ramp is selected by chance alone.

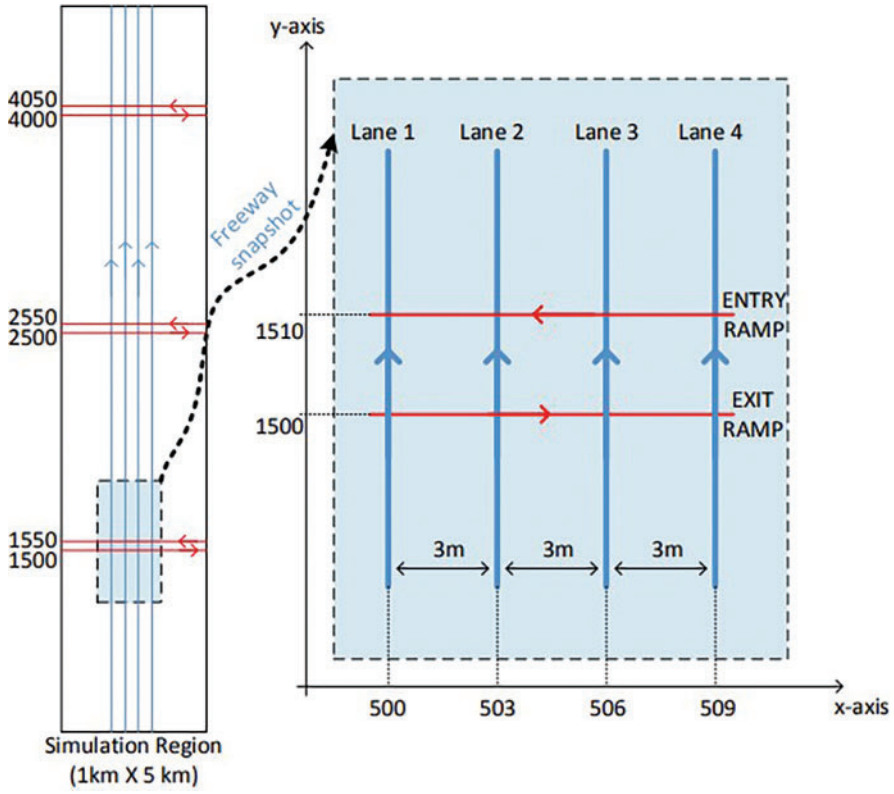

Figure 6: Simulated four-lane

4.2 Vehicle-To-Vehicle (V2V) Broadcasting

Vehicle-to-vehicle (V2V) broadcasting of safety warnings with a transmission range of 50 m results in the network data traffic. It is also possible to employ a non-safety application in which vehicles are required to join a group of nodes connected by V2V for a short period (seconds or less). As a result of these network applications, the following two simulation settings have emerged: Fig. 7 shows 3 automobiles are simulated on the user's two crossing roadways, a vehicle's radio communication range is 50 m, and Fig. 8 shows 3 automobiles are simulated on the user's two crossing roadways the simulation iteration step must be at least 100 milliseconds by using the AVISPA Tool.

An example of a simulator's generated visual interface for taking user input and visualizing the results is depicted in Figs. 9–11 by using the AVISPA Tool. 3 automobiles are simulated on the user's two crossing roadways, each traveling randomly and approaching the intersection. While moving, V2V linkages form between nodes that are within radio communication range. Some V2V linkages fail as nodes travel towards the end of the roads and are no longer in communication range.

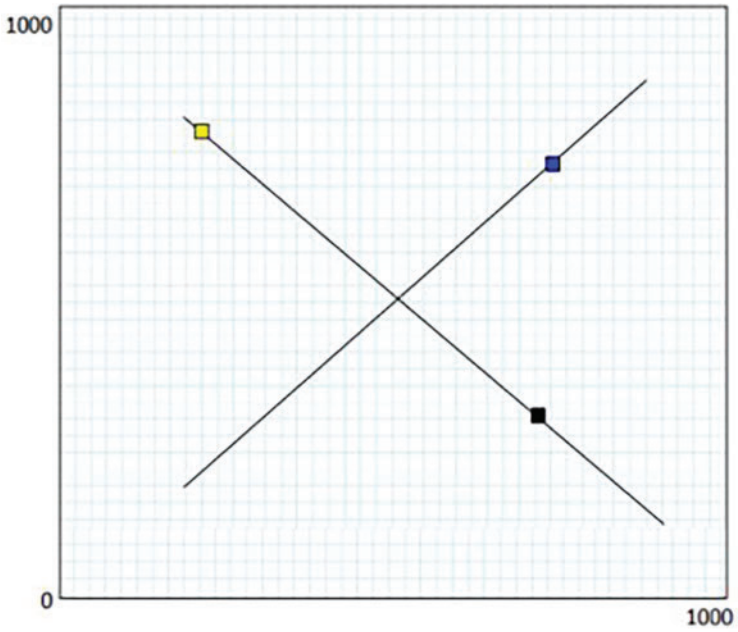

Figure 7: 3 automobiles are simulated on the user's two crossing roadways

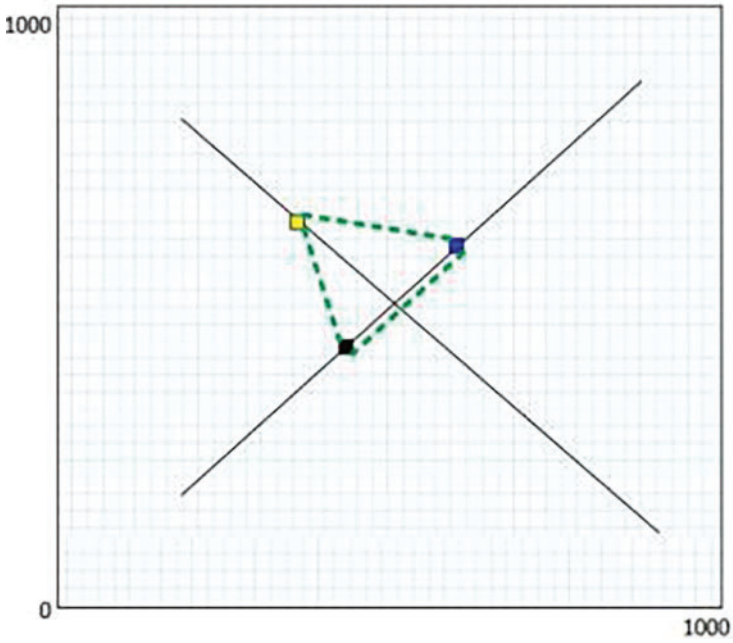

Figure 8: 3 automobiles are simulated on the user's two crossing roadways

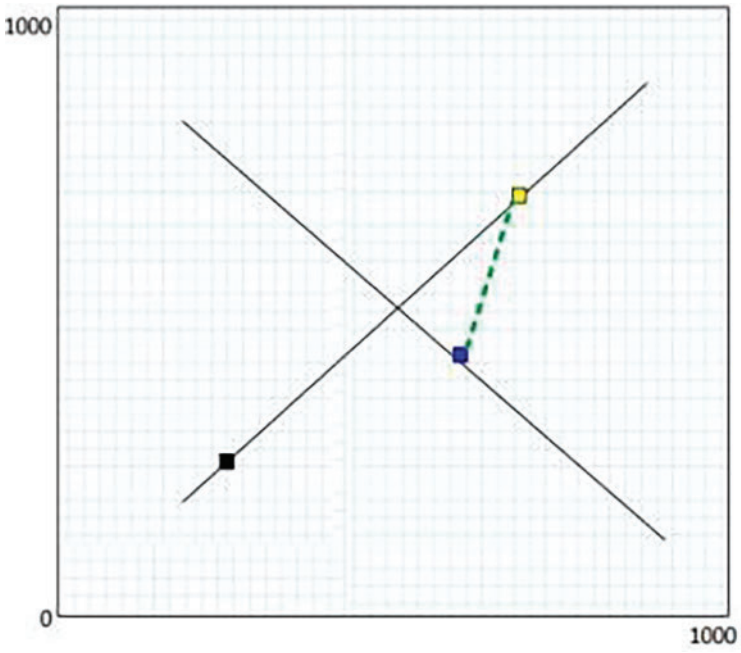

Figure 9: 3 automobiles are simulated on the user's two crossing roadways

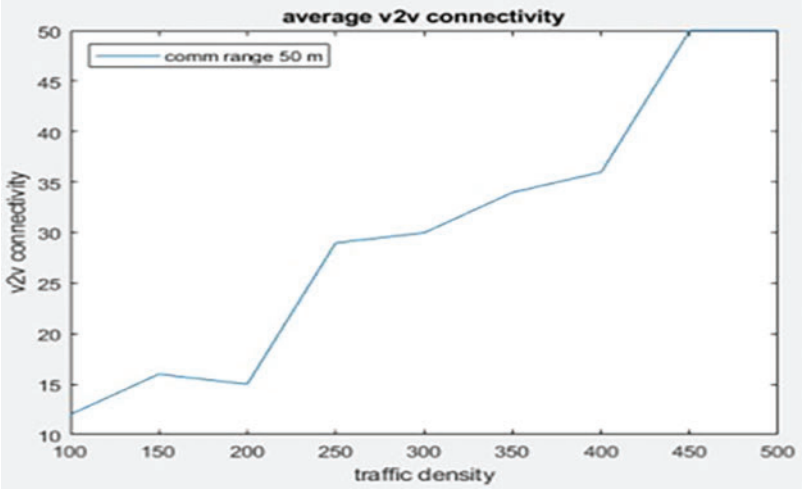

Figure 10: Average V2V connectivity

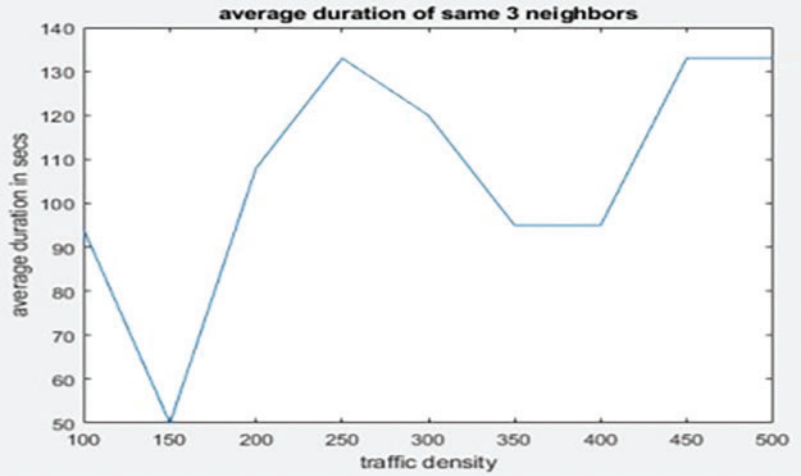

Figure 11: Average duration of same 3 neighbors

4.3 VANET Visualization and Assessment Tool Simulation

We'll build a high-level simulator to see how V2V and V2I communication works on roads and freeways in this simulation. Advanced networking and wireless analysis should not be done using the simulator's output. However, it is up to you to be innovative and design this simulation tool so that a user can grasp V2V and V2I communication and the associated applications and issues. There are two sections to this design: A 4-way road intersection with user-provided V2V connectivity may be visualized and assessed. V2I coverage difficulties for a user-provided road and RSU deployment can be visualized and assessed. Both of these sub-parts can be entered into the Mat lab using the input function.

4.4 Discussion

When developing a vehicular hoc network with V2V and V2I connectivity, it's critical to keep vehicular mobility in mind. Initially, this project will look at how vehicle mobility and traffic volume affect vehicle-to-vehicle connectivity. The freeway mobility model, the lane changing model, and the border effects are all effectively implemented in Matlab for a 4-lane scenario with three entry ramps and three exit ramps. For each traffic density, the simulations run for five trials of ten minutes each. Based on our graphs, these figures appear possible and practical, which show linear variation with increasing traffic density. The output changed when the communication range shifted. The charts that follow represent the results of five simulations, each of which was performed for five minutes. The distance at which you can communicate is 50 m.

1. The plot shows the average number of communication nodes within 50 m of the target.
2. The plot shows the average duration the target node maintains the same 3 communication neighbors that are within 50 m.
3. The plot shows the average number of the same neighbors for 30 s.

Fig. 10 shows that, as expected, the average duration of the same three neighbors grows linearly with traffic density. The same neighbors tend to stay together longer as traffic intensity increases. Because of the congestion in other lanes, drivers change lanes less frequently, reducing the risk of

being out of sight. As traffic congestion increases, the duration varies from 1 min to 6 min. As a result, we can use this approach to send data that isn't life-threatening.

Plots at 50 m and 100 m are shown in the figures below. Two minutes worth of simulations are run on a 50 m and 100 m course. The charts show the differences when the communication range is increased to 100 m, which is the result of five simulations for each. A bar graph depicts the average number of communication nodes within 50 and 100 m of the target in red and blue, respectively.

The plot shows the average duration the target node maintains the same communication neighbors that are within 50 m (red) and 100 m (blue). The plot shows the average number of the same neighbors for 30 s for 50 m (red) and 100 m (blue) communication ranges.

As traffic density rises, so does the number of neighbors, as cars are forced to cram themselves closer together to avoid collisions. As a result, traffic density has a linear effect on average V2V connectivity. When uniformly deployed, each node has connectivity with 8–40 vehicles when considering 100–500 vehicles in a lane of 5 km and a communication range of 50 m. The data in each of our graphics is identical. Abnormalities in the graphs don't happen at the same density every time; they happen at random. Perhaps this is the case because the random distribution of speed and distance changes every 100 m/s, making the simulation unpredictable even when using average values. The average time of three neighbors at a specific period grows linearly with traffic density, as seen in Fig. 10. Congestion and a reduced ability to change lanes would be caused by increased traffic, as explained previously. The average number of neighbors increases from 4 to 40 in 30 s. Figs. 10–14 show a comparison of plots from 100 m and 50 m. It's easy to observe that the outcomes have nearly doubled.

V2V Connectivity of Approaching Vehicles at 4-Way Road Intersection Simulation. When the user sketches two roads that connect, three random automobiles begin to move toward the intersection at random speeds.

1. A connection is established if the distance between the vehicles is less than 100 m. The connection is shown by the green dashed line.
2. Connection is established between all three vehicles when they are close to the intersection.

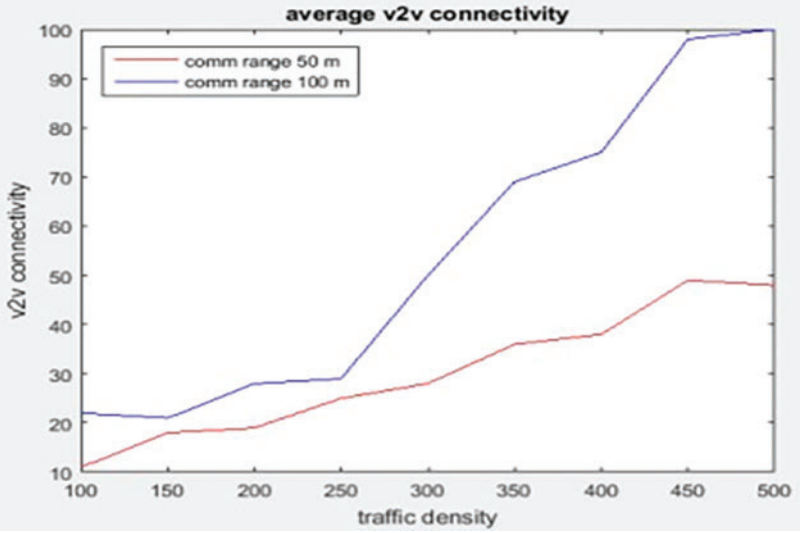

Figure 12: Average V2V connectivity

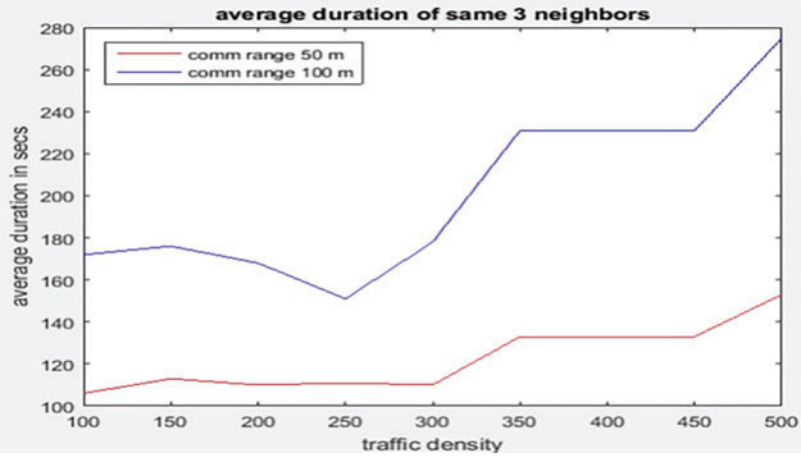

Figure 13: Average duration of same 3 neighbors

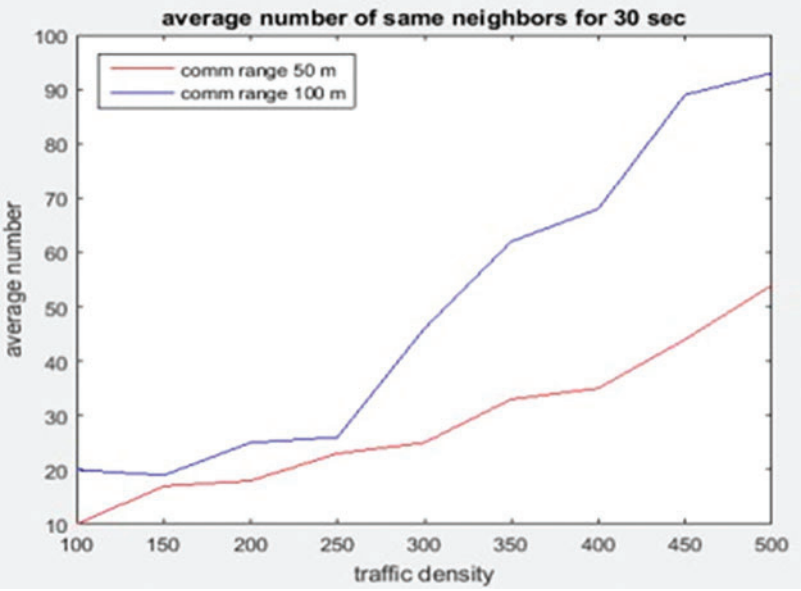

Figure 14: Average duration of 3 neighbors for 30 s

The user creates three roadways and sets two RSUs on each one. A connection is established if the distance between the vehicle and any RSU is less than 100 m. Paths with no connections are shown in red, whereas paths with connections are shown in green. The figure below shows the coverage of the simulation for a car with average V2V connectivity.

Fig. 15 shows connection is established if the distance between the vehicles is less than 100 m. The connection is shown by the green dashed line. Fig. 16 shows the coverage of the simulation for a car with average V2I connectivity.

Fig. 17 shows V2I Connectivity. This connection is established between all three vehicles when they are close to the intersection.

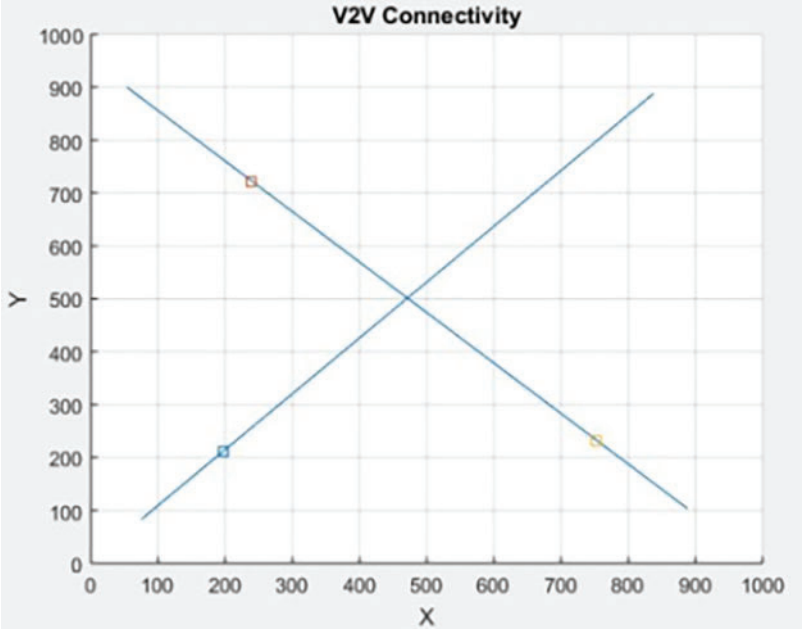

Figure 15: Connection is established if the distance between the vehicles is less than 100 m

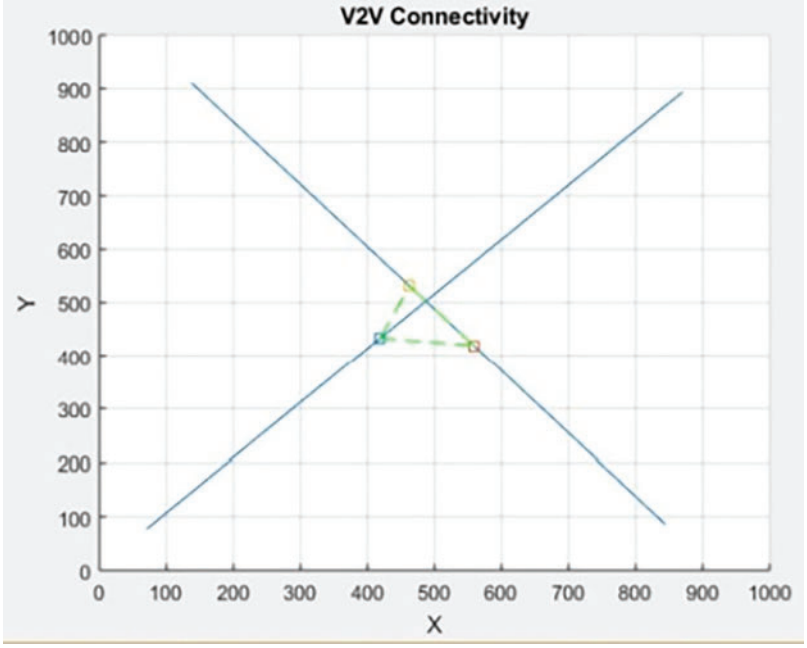

Figure 16: The coverage of the simulation for a car with average V2I connectivity

The user creates three roadways and sets two RSUs on each one. A connection is established (see Fig. 18) if the distance between the vehicle and any RSU is less than 100 m. Paths with no connections are shown in red, whereas paths with connections are shown in green.

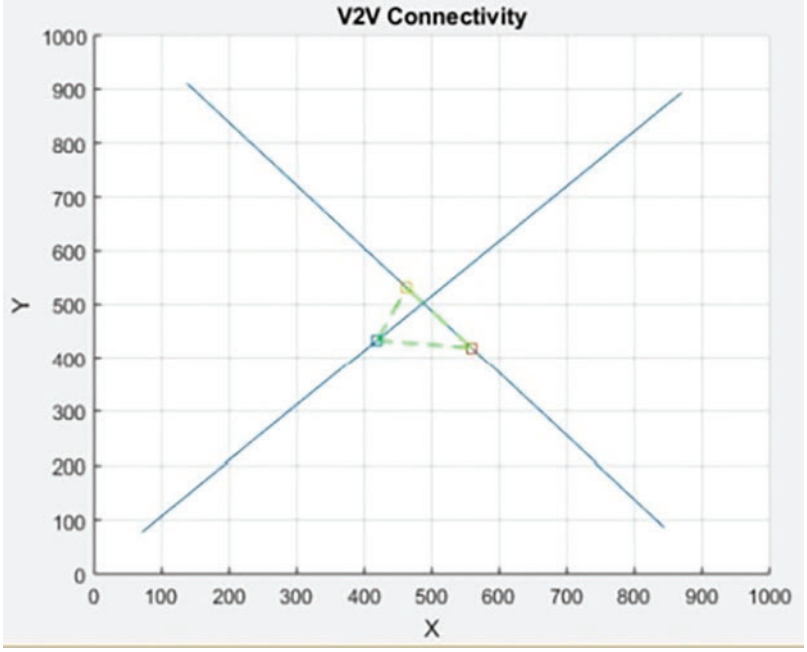

Figure 17: V2I connectivity

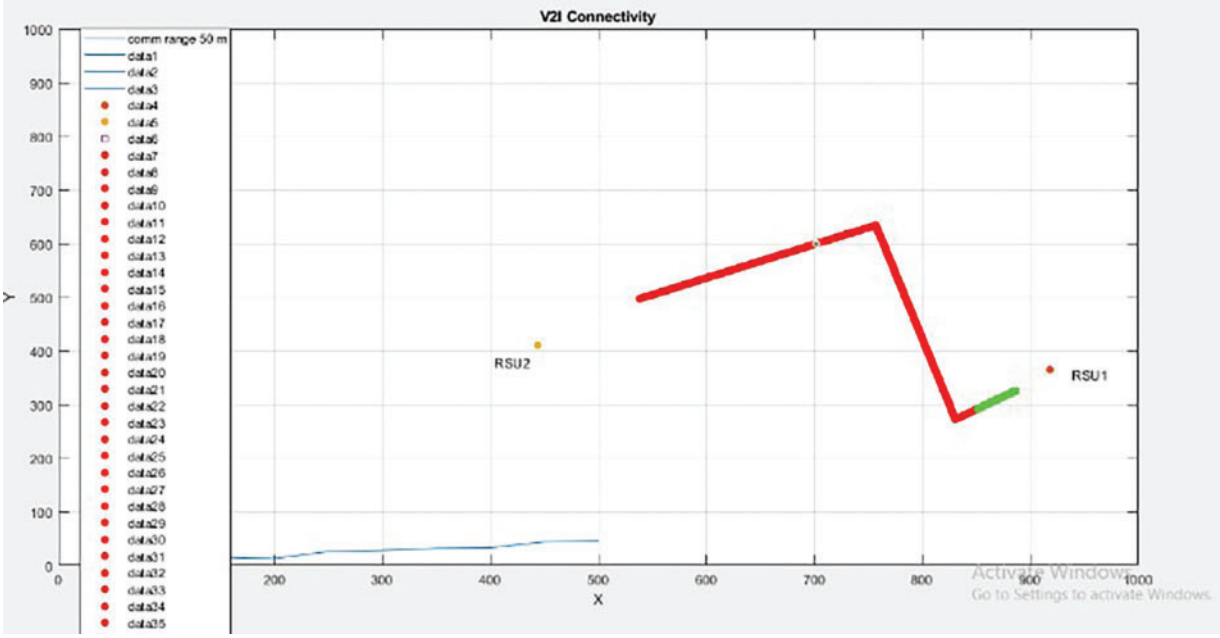

Figure 18: V2I connectivity

5 Conclusions

Security in Intelligent Transport Systems (ITS) by using advanced blockchain-based authentication protocol. Integrating computer technology and the Internet of Things (IoT) in the automotive

sector has significantly improved life, with transport and logistics reaping the benefits of these advancements. However, the increasing number of road accidents globally, coupled with the pervasive use of high-traffic websites, underscores the urgent need for robust solutions to enhance road safety and mitigate accidents' impact. The implementation of contemporary communication technologies, such as front sensors, controllers, and actuators, has revolutionized the automotive sector, enabling seamless transactions and information exchange between vehicles and their surroundings. This technological integration empowers vehicles to comprehend their environments, make informed decisions, and engage in co-management processes. Leveraging the Internet of Things in vehicles not only prevents accidents but also introduces features like intelligent automation, large data management, shared data utilization, intelligent navigation, and connectivity with mobile devices. Despite these advancements, concerns related to data privacy and security in the Internet of Vehicles (IoV) persist as well. As vehicles become increasingly connected, the submission of sensitive information by drivers raises the risk of data breaches and privacy infringements. This study recognizes the need for a comprehensive and secure authentication system to protect user privacy, prevent data leakage, and ensure overall safety. The economic implications of implementing blockchain and smart transport are significant, necessitating a thorough cost-benefit analysis for governments and corporations. Blockchain technology, with its emphasis on transparency and trust, offers a pathway to low-cost corporate environments, mitigating business instability through smart contracts and advanced data management techniques. Moreover, the integration of blockchain with IoT facilitates real-time data integration and transfers, reducing processing time and fostering secure and reliable agreements. This research addresses the importance of blockchain and IoT in ensuring Internet traffic protection. The integrity of vehicle and device data is paramount, and measures to protect user privacy must be prioritized within the automotive sector. The study acknowledges the challenges posed by the rapid growth of automotive applications and services, emphasizing the need for a decentralized, distributed, interoperable, and scalable infrastructure for the secure, private, and trustworthy transmission and storage of IoV data. In summary, the proposed blockchain-based authentication protocol for Intelligent Transport Systems represents a significant step toward creating a safer, more efficient, and privacy-preserving vehicular communication environment. The real-world performance evaluation of the model confirms its effectiveness, paving the way for the adoption of blockchain technology as a key enabler in the evolution of Intelligent Transport Systems.

Acknowledgement: We thank Awad Bin Naeem (NCBA&E) for writing the research article evaluation, simulation work in SUMO, paper methodology, and paper conceptualization. Biswaranjan Senapati (Parker Hannifin Corp.) provided software assistance, while Abdelhamid Zaidi (Qassim University) reviewed and modified the paper in response to journal reviews and simulation work. Satyabrata Pradhan (General Motors, Warren) assisted with the investigation and methodology of the work. Pakistan and the United States Transportation System contributed to this study.

Funding Statement: This research received no external funding.

Author Contributions: Muhammad Imran Ghafoor: Conceptualization, Methodology. Awad Bin Naeem: Methodology, Software, Writing study, Writing review and editing. Biswaranjan Senapati: Data curation, Writing—original draft preparation. Md. Sakiul Islam Sudman: Software, Field study. Satyabrata Pradhan: Software and Writing. Debabrata Das: Review and Editing. Friban Almeida: Software. Hesham A. Sakr: Investigation and Methodology. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors declare that all data supporting the findings of this study are available within the article.

Ethics Approval: Not applicable.

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

References

[1] Y. Cui *et al.*, "Deep learning for image and point cloud fusion in autonomous driving: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 2022, no. 23, pp. 722–739, 2022. doi: 10.1109/TITS.2020.3023541.

[2] G. Bosurgi, D. Bruneo, F. De Vita, O. Pellegrino, and G. Sollazzo, "A web platform for the management of road survey and maintenance information: A preliminary step towards smart road management systems," *Struct. Control Health Monit.*, vol. 29, no. 3, 2022, Art. no. e2905. doi: 10.1002/stc.2905.

[3] M. Moradi and G. J. Assaf, "Designing and building an intelligent pavement management system for urban road networks," *Sustainability*, vol. 15, no. 2, 2023, Art. no. 1157. doi: 10.3390/su15021157.

[4] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May–Jun. 1, 2022. doi: 10.1109/TNSE.2022.3142287.

[5] A. B. Naeem, A. M. Soomro, H. M. Saim, and H. Malik, "Smart road management system for prioritized autonomous vehicles under vehicle-to-everything (V2X) communication," *Multim. Tools Appl.*, vol. 83, no. 2023, pp. 41637–41654, 2023. doi: 10.1007/s11042-023-16950-1.

[6] A. Di Febbraro, F. Gallo, D. Giglio, and N. Sacco, "Traffic management system for smart road networks reserved for self-driving cars," *IET Intell. Transp. Syst.*, vol. 14, no. 9, pp. 1013–1024, 2020. doi: 10.1049/iet-its.2019.0675.

[7] A. Sharma, Y. Awasthi, and S. Kumar, "The role of blockchain, AI, and IoT for smart road traffic management system," in *2020 IEEE India Council Int. Subsections Conf. (INDISCON)*, Visakhapatnam, India, 2020, pp. 289–296. doi: 10.1109/INDISCON50162.2020.00065.

[8] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019. doi: 10.1109/TVLSI.2019.2929420.

[9] T. Nandy *et al.*, "A secure, privacy-preserving, and lightweight authentication scheme for VANETs," *IEEE Sens. J.*, vol. 21, no. 18, pp. 20998–21011, Sep. 15, 2021. doi: 10.1109/JSEN.2021.3097172.

[10] R. Horowitz and P. Varaiya, "Control design of an automated highway system," *Proc. IEEE*, vol. 2000, no. 88, pp. 913–925, 2000. doi: 10.1109/5.871301.

[11] S. M. Grigorescu, B. Trasnea, T. T. Cocias, and G. Macesanu, "A survey of deep learning techniques for autonomous driving," *J. Field Robot*, vol. 2020, no. 37, pp. 362–386, 2020. doi: 10.1002/rob.21918.

[12] P. Dai, K. Liu, Q. Zhuge, E. H. M. Sha, V. C. S. Lee and S. H. Son, "Quality-of-experience-oriented autonomous intersection control in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, pp. 1956–1967, 2016.

[13] K. Gao, S. Huang, J. Xie, N. N. Xiong, and R. Du, "A review of research on intersection control based on connected vehicles and data-driven intelligent approaches," *Electronics*, vol. 9, no. 6, 2020, Art. no. 885. doi: 10.3390/electronics9060885.

[14] J. Fayyad, M. A. Jaradat, D. Gruyere, and H. Najjaran, "Deep learning sensor fusion for autonomous vehicle perception and localization: A review," *Sensors*, vol. 20, no. 15, 2020, Art. no. 4220. doi: 10.3390/s20154220.

[15] B. Ji and E. J. Hong, "Deep-learning-based real-time road traffic prediction using long-term evolution access data," *Sensors*, vol. 19, no. 23, 2019, Art. no. 5327. doi: 10.3390/s19235327.

[16] P. A. Hancock, I. Nourbakhsh, and J. Stewart, "On the future of transportation in an era of automated and autonomous vehicles," *Proc. Natl. Acad. Sci. USA*, vol. 2019, no. 116, pp. 7684–7691, 2019. doi: 10.1073/pnas.1805770115.

[17] K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller and H. Winner, "Three decades of driver assistance systems: Review and future perspectives," *IEEE Intell. Transp. Syst. Mag.*, vol. 6, pp. 6–22, 2014.

[18] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, 2019, Art. no. 101823. doi: 10.1016/j.adhoc.2018.12.006.

[19] M. Rath, "Smart traffic management system for traffic control using automated mechanical and electronic devices," IOP Conf. Ser.: Mater. Sci. Eng., vol. 377, 2018, Art. no. 012201. doi: 10.1088/1757-899X/377/1/012201.

[20] M. A. Islam and S. I. Rashid, "Algorithm for ethical decision making at times of accidents for autonomous vehicles," in *Proc. 2018 4th Int. Conf. Electr. Eng. Inf. & Commun. Technol. (iCEEiCT)*, Dhaka, Bangladesh, Sep. 13–15, 2018, pp. 438–442.

[21] S. Tangade and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," in *Proc. 2016 IEEE Int. Conf. Adv. Netw. Telecomm. Syst. (ANTS)*, Bangalore, India, Nov. 6–9, 2016, pp. 1–6.

[22] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 2018, no. 5, pp. 3701–3709, 2018. doi: 10.1109/JIOT.2017.2690902.

[23] P. Tientrakool, Y. -C. Ho, and N. F. Maxemchuk, "Highway capacity benefits from using vehicle-to-vehicle communication and sensors for collision avoidance," in *Proc. 2011 IEEE Veh. Technol. Conf. (VTC Fall)*, San Francisco, CA, USA, Sep. 5–8, 2011, pp. 1–5.

[24] G. R. Nookala Venu, K. Maneesha, K. Anusha, S. Merugu, and A. Mohammad, "Smart road safety and vehicle accidents prevention system for mountain road (July 2022)," *Int. J. Innov. Eng. Manag. Res. (IJIEMR)*, vol. 11, no. 6, pp. 209–214, Jul. 2022.

[25] Q. Xie, Z. Ding, W. Tang, D. He, and X. Tan, "Provable secure and lightweight blockchain-based V2I handover authentication and V2V broadcast protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 15200–15212, Dec. 2023. doi: 10.1109/TVT.2023.3289175.