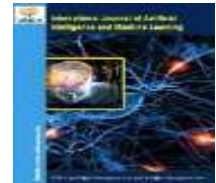




SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

An Integrated SDN–Blockchain Framework for Secure and Intelligent Communication in IoT-Enabled Vehicular Networks

Nishigandha Manohar Pachore¹, Dr. Satish M. Turkane²

¹Research Scholar, Jai Hind College of Engineering, Narayangaon, Email - nmp2293@gmail.com

²E&TC Dept. PREC Ioni, Email- satish.turkane@gmail.com

ABSTRACT

Intelligent transportation systems are increasingly relying on connected vehicles and Internet of Things (IoT) technologies to improve road safety, traffic efficiency, and real-time communication. Ensuring secure, reliable, and low-latency communication in highly dynamic vehicular environments remains a significant challenge due to frequent topology changes, high vehicle mobility, and growing cybersecurity threats. Conventional Vehicular Ad Hoc Networks (VANETs) often experience limitations in network management, resource utilization, and trust establishment, reducing their ability to support critical applications such as emergency vehicle communication. This study proposes an integrated Software-Defined Networking (SDN) and blockchain framework to provide intelligent network control and secure communication for IoT-enabled vehicular networks. The proposed framework employs a centralized SDN controller for dynamic Road Side Unit (RSU) allocation, adaptive routing, and priority-based communication, while blockchain technology ensures transaction authentication, data integrity, and decentralized trust using SHA-256 hashing and a lightweight Proof-of-Work consensus mechanism. The framework was implemented in Python with a Flask-based web dashboard and evaluated through simulation using network performance and blockchain metrics. The results demonstrate stable vehicle–RSU connectivity, efficient routing, successful blockchain transaction validation, and reliable priority communication for emergency vehicles. These findings demonstrate that integrating SDN with blockchain improves communication efficiency, network security, and resource utilization compared with conventional approaches. The proposed framework provides a scalable foundation for secure next-generation intelligent transportation systems and offers opportunities for future enhancement through distributed SDN controllers, lightweight blockchain consensus mechanisms, and edge computing integration.

Keywords: Software-Defined Networking (SDN), Blockchain, Internet of Things (IoT), Vehicular Ad Hoc Networks (VANETs), Intelligent Transportation Systems (ITS), Road Side Units (RSUs), Priority-Based Communication.

1. Introduction

The development of modern digital communication technologies has led to a change in the functioning of transportation systems, as a result of which there is real-time exchange of data between vehicles, infrastructure, and traffic control services [1]. It should be noted that modern transportation cannot be regarded as mere transportation of cars from one point to another but represents an intelligent system of traffic optimization, road safety, emergency response, and self-driving applications [2]. Due to the growing number of connected cars and the advent of smart cities, there has been an increasing need for communication technologies capable of providing secure, reliable, and low-latency communication in highly dynamic networks [3]. Efficient communication between vehicles and roadside infrastructure will help minimize traffic congestion, prevent road accidents, and increase efficiency within the transportation networks [4]. It has therefore become one of the major research concerns within the next generation of transportation systems [5]. With the integration of communication technologies in computing and networking, vehicles have become smart entities that are able to sense, process, and exchange information regarding their present status [6]. Connected cars share information concerning their locations, speed, traffic conditions, and emergencies to arrive at a joint decision for managing traffic [7]. Furthermore, the advent of the concept of Internet of Things (IoT) has reinforced this idea wherein physical objects with sensors and communication capabilities are interacting within networking environments [8]. In the case of intelligent transportation systems, IoT allows for establishing permanent connections between vehicles, roadside facilities, and management systems [9]. But the dynamism of vehicular networks poses many challenges, which include frequent changes in topologies, connectivity issues, communication delays, resource utilization, and security risks. Solutions to such problems need intelligent network management solutions that can adapt to constantly varying traffic conditions to ensure effective communication performance [10].

However, to address such limitations, scientists have started investigating modern network security solutions capable of offering centralized control, efficient resource management, and secure communications [11]. The concept of Software-Defined Network (SDN) allows implementing a centralized network management solution where control operations can be separated from the data forwarding equipment and thus enables the network

to operate dynamically based on variations in the mobility and communication requirements of vehicles [12]. Simultaneously, the distributed nature of blockchain technology allows implementing data integrity, authentication, and trust between the communicating parties without the need for any single trusted party [13]. The combination of SDN with blockchain technology can be used to provide a robust approach that uses both intelligent network control and security of data storage for better communication within connected transportation networks [12]. With this in mind, this paper aims to present an integrated SDN-blockchain system that would allow secure and intelligent communication within vehicular IoT networks via intelligent network management and network monitoring [14].

Intelligent transportation systems' rapid proliferation in today's era has made the need felt for a communication protocol framework capable of providing security, reliability, and efficiency to data communication among these connected vehicles. But the existing vehicular communication network architecture is faced with many limitations such as dynamic changes in network topology, latency issues, poor utilization of resources, and increased security concerns. This research paper focuses on the development of an integrated SDN-blockchain framework for securing IoT-enabled vehicular networks. The proposed model integrates the centralization aspect of SDN in networking with the decentralization of blockchain to enhance efficiency, reliability, and scalability of the network communications. The main aim of this research study is to develop a new communication model that will help to manage vehicular mobility, provide appropriate allocation of Road Side Units (RSUs), give priority to emergency vehicle communications, and ensure transactional security by means of blockchain. The above-stated aims have been fulfilled by creating a simulation environment using Python, Flask, NetworkX, and Plotly.

The proposed study uses a simulation-based approach where a realistic environment of the highway with several lanes, cars, and RSUs is simulated to reflect actual vehicular communication situations. The SDN controller controls the network in a centralized manner by monitoring the current state of the network and allocating RSUs accordingly to vehicle movement and communication needs. At the same time, the blockchain system logs communication transactions in an unalterable way by using the lightweight Proof-of-Work consensus algorithm. The scope of the current research is restricted to the implementation and testing of a secure SDN-blockchain-based communication protocol in a simulated IoT-enabled vehicular scenario. Though the designed model proves to be an efficient and secure communication protocol, its practical implementation and integration with edge computing technology are something to be investigated in the future.

The main novel aspect of the study is that of a combination of centralized SDN-based network management and decentralized blockchain-based security in one vehicular communication system. In contrast to many other studies that analyze routing optimization, network security, and/or blockchain implementation separately, the proposed system takes into consideration such important aspects as dynamic RSU allocation, emergency vehicle priority, transaction validation, and network monitoring using a web-based interactive dashboard. The rest of this paper is structured as follows. Section 1 proceeds from the background of the study. Section 2 gives a review of the literature and determines the research gap. Section 3 introduces the proposed SDN-blockchain framework and architecture of the system. Section 4 outlines the implementation procedure and experiment design. The results of the simulation are described in Section 5. Finally, Section 6 concludes the research, and future work perspectives are suggested.

2. Literature Review

The rapid evolution of intelligent transportation systems (ITS) has brought revolutionary changes in vehicular communication, enabling vehicles, roadside infrastructure, and traffic control systems to communicate with each other in real time. Connected vehicles have increased efficiency, safety, and the driving experience because of constant communication between intelligent transportation system components. The dynamics of the vehicular environment, which includes changing topology, high mobility of vehicles, intermittency of communication, and heterogeneity of communication needs, create substantial obstacles to achieving secure and reliable communication. This is why research work has been directed towards creating intelligent networks that would be able to provide adaptive routing, effective resource allocation, low communication latency, and scalability of the network.

Vehicle Ad hoc Networks (VANETs) have become one of the key technologies facilitating modern transport systems. VANET facilitates vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I), providing the ability for vehicles to exchange safety messages, traffic updates, and emergency notifications. However, traditional VANET architecture is characterized by decentralization of routing, low network awareness, poor traffic management, and susceptibility to cyber attacks. All the mentioned aspects are especially critical for a dense urban environment where reliable communication and effective use of network resources are very difficult. To overcome these problems, Software-Defined Networking (SDN) was offered as a new approach, which allows separation of the control plane and data plane of the network and provides centralized network intelligence and traffic management. It was shown by recent surveys that SDN significantly enhances the routing efficiency and communication performance in vehicular environments [15].

Apart from intelligent networking, secure communication is also another significant aspect that needs to be

considered in vehicular networks. The application of blockchain technology has become quite popular in recent times due to its unique features such as decentralization, immutability, and consensus, which provide more assurance of data integrity and trust without any central authority. Edge computing is also becoming popular in the field of intelligent transportation systems for minimizing communication latency through processing the data near the vehicle. Recent research indicates that an integration of SDN, blockchain, and edge computing will enable a solution to be developed for issues related to security, scalability, resource allocation, and real-time communication. Nonetheless, even though several efforts have already been made in developing each technology and considering some specific aspects such as route optimization, security improvement, or controller design, many opportunities still exist for the development of a comprehensive communication framework[16].

Dwivedi et al. conducted an extensive review of the applications of blockchains in Vehicular Ad Hoc Networks to examine the possible benefits that could be derived from blockchain technology with respect to enhancing communication security, privacy, authentication and trust management in intelligent transport systems. Various blockchain technologies, consensus mechanisms, and vehicle application domains have been analyzed in terms of their performance under different communication scenarios. It has been observed that there are significant benefits of using blockchains to improve decentralization of authentication, secure information exchange, and traceability without relying on any central authority. There are some challenges associated with this aspect, including high computation costs, high latency in consensus process, scalability issues, and integration into existing vehicular communication mechanisms [17].

Khajeh et al. reviewed the topic of SDN and Blockchain for vehicular communication network comprehensively, studying the connection between central network management and decentralized security. The authors analyzed the architecture, routing, trust management, and security protocols within intelligent transportation systems. It has been found that SDN provides a solution to centralized traffic control and adaptive routing whereas Blockchain provides reliable communication via transaction logging. Even though the combination of both technologies significantly enhances communication efficiency and security, some problems were noted, such as the scalability of controllers, blockchain overhead, interoperability, and real-time operation. It was advised to develop such integrated frameworks that could provide efficient and trustworthy communication at the same time [18].

Table 1. Comparative Analysis of Recent Studies on SDN, Blockchain, and Vehicular Networks

Study	Method	Key Findings	Limitations
Dwivedi et al. [17]	Blockchain-enabled VANET architecture	Improved authentication, privacy, and decentralized trust management	High computational overhead and blockchain scalability issues
Varma et al. [18]	SDN-Blockchain integrated survey	Enhanced secure communication through SDN and blockchain integration	Lack of practical implementation and real-time validation
Hussein et al. [15]	SDN-based routing survey	Centralized SDN improves routing efficiency and resource management	Controller scalability and routing overhead remain unresolved
Nurkahfi et al. [19]	SDN architecture for IEEE 802.11p and C-V2X	Improved network flexibility and communication reliability	Limited interoperability among heterogeneous vehicular networks
Ul Haq et al. [16]	SDN-enabled edge computing framework	Reduced latency and improved resource utilization	Controller coordination and edge resource optimization require further investigation
Sarpong et al. [20]	SDN with multihoming for VANETs	Increased communication reliability using multiple communication interfaces	Complex routing management and increased implementation complexity
Almutairi et al. [21]	VANET simulation platform review	Comprehensive comparison of simulation platforms	Existing simulators provide limited security and blockchain integration capabilities
Proposed Study	Integrated SDN-	Centralized SDN	Simulation-based

	Blockchain Framework with Dynamic RSU Allocation	management, secure blockchain-based communication, priority-aware emergency vehicle communication, real-time monitoring, and dynamic RSU allocation	evaluation; future work includes large-scale deployment, distributed SDN controllers, and edge computing integration
--	--	---	--

2.1. Research Gap

The current state-of-the-art research reveals that there has been remarkable progress in integrating SDN, blockchain technology, and edge computing into intelligent vehicular communications. Many works have examined the application of SDN towards centralized network control, flexible routing, and optimal resource allocation. In addition, many research efforts have concentrated on the application of blockchain technology to provide secure authentication, trust management, and reliable storage. Moreover, edge computing has been employed to address the issue of reducing communication delays and enabling real-time applications. Nonetheless, the current research works consider each of the above technologies independently or a particular aspect of the technology, such as routing, security, placement, and computation offloading.

Additionally, most of the methods proposed up till now lack the consideration of not only dynamic allocation of RSUs but also that of traffic prioritization of emergency vehicles, blockchain-based transaction validation, and network monitoring in the same simulation setting. Scalability of the controller, computational overhead involved in blockchain operations, lightweight consensus, compatibility among heterogeneous communication technologies, and coordination among SDN controllers and vehicular infrastructures have remained as open problems.

To overcome such limitations, the current study provides an integrated solution using SDN and blockchain in IoT-based vehicular networks for reliable and intelligent communication. In this regard, a framework comprising centralized SDN-based network management along with decentralized blockchain-based security has been designed to provide dynamic allocation of RSUs, priority-based communication for emergency vehicles, secure record-keeping of transactions, and performance monitoring through a web-based dashboard interface. Through this integration of such capabilities within one simulation environment, it is expected that many of the research gaps revealed by recent studies would be addressed.

3. Methodology

The proposed methodological approach introduces an integrated communication model that incorporates both SDN and blockchain technologies into a framework to create a secure, reliable and intelligent communication environment for the IoT-enabled vehicular networks. This framework is designed to resolve some of the problems encountered in conventional VANET frameworks, which include dynamic topology, network management inefficiencies, delay in communication, and security issues. By virtue of employing centralized network intelligence and decentralized security framework, the proposed framework ensures effective communication between vehicles, RSU nodes, and network infrastructure.

The deployment process begins with the creation of a virtual highway with several lanes, the correct positioning of RSUs, and different kinds of vehicles that include regular vehicles and emergency vehicles such as ambulance, firefighting truck, and police car. The Network Manager is responsible for performing network initialization, vehicle mobility management, communication settings, and overall simulation process management. Traditional distribution routing algorithms require manual involvement for carrying out the process, but the methodology suggested in the paper requires the use of SDN controller that monitors the communication environment, initializes the network topology, and assigns the best suited RSU for each vehicle based on communication range and priority. The emergency vehicles have been allocated a higher communication priority level than the rest of the vehicles.

To ensure that communication security is improved, blockchain technology is embedded in the communication system. Every significant event in the network, such as registering vehicles, associating RSUs, and communicating, is made a transaction on the blockchain. Each of the transactions is then authenticated using the SHA-256 algorithm and validated using a lightweight Proof-of-Work protocol and added to the blockchain database. This guarantees data storage, decentralized trust management, and communication transparency. Moreover, the entire simulation is tracked using a Flask web dashboard via REST API interfaces. The methodology proposed above hence gives a unified solution for intelligent traffic communication since it includes SDN management, blockchain technology for securing communication, and interaction with the network in one simulation platform.

3.1. Proposed Framework

This framework provides a combined SDN and blockchain based communication framework for secure and intelligent communication in the context of IoT-enabled vehicular networks. This framework includes a simulation setup of highway with several RSUs, connected vehicles, centralized SDN controller, and a

blockchain component. This SDN controller takes care of dynamic management of network topology, vehicle mobility, RSU placement, and priority to emergency vehicle communication. Meanwhile, blockchain technology ensures security of transaction, data integrity, and decentralization of trust through immutable data storage. The core purpose of this framework includes improved communication performance, security, resource management, and real-time network monitoring using web-based interactive dashboard.

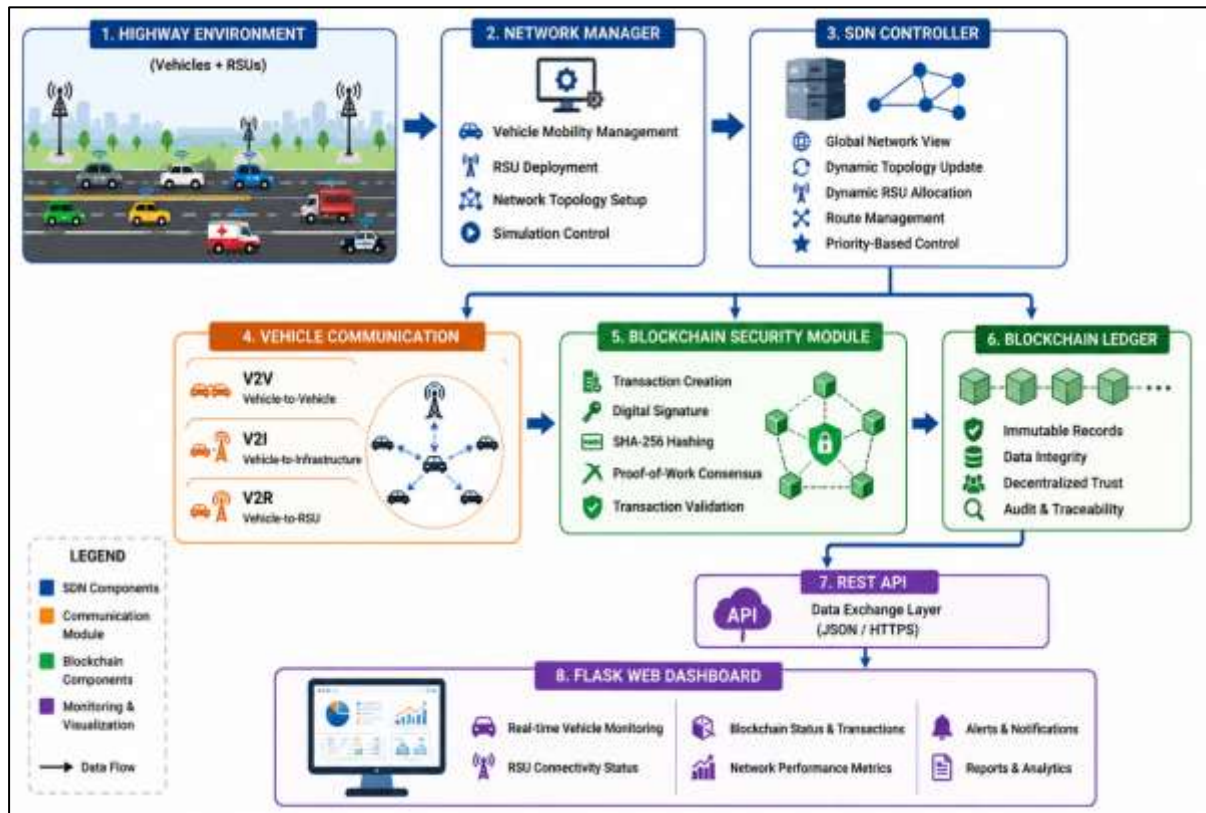


Figure 1.SDN-Blockchain System Architecture

3.2. System Model

This system model is an integration of SDN with blockchain technology into a communication system for IoT-driven vehicle networks. The communication system has been implemented using a simulated highway setup, which consists of a road with multiple lanes and where the movement of vehicles is dynamic based on certain mobility models. There are several RSUs installed on the road to provide connectivity among vehicles and the communication network. The network consists of different types of vehicles such as normal vehicles and emergency vehicles with certain communication priorities.

The Network Manager is responsible for the initialization of the simulation environment through the creation of the vehicles, the deployment of the RSUs, the network topology maintenance, and the management of the vehicle movement throughout the simulation process. The SDN Controller is responsible for the monitoring of the network conditions, the updating of the communication topology, the management of the RSU associations, and the intelligent routing of data transmission to guarantee an efficient and reliable data transfer. In order to enhance the security of the communications, the Blockchain Module creates blocks on the blockchain that record the vehicles' registrations, the communication events, and the routing of the data transmission. This module utilizes the SHA-256 hashing algorithm and a lightweight Proof-of-Work mechanism to verify the transactions.

3.3. Network Initialization

Network initialization is the process whereby the network simulation environment is set up by defining all the communication elements before any data transfer takes place. Initially, a highway setting is established with various lanes to enable a real-world scenario for vehicle transportation. The dimensions of the road, number of lanes, and movement range is established to enable smooth movement of vehicles in the simulation. Afterward, several Road Side Units (RSUs) are established in the highway with a certain communication range to allow V2I communication.

After the network infrastructure is set up, various types of vehicles with specific speed, orientation, and priority characteristics are randomly generated. All vehicles have unique identification details and mobility details to replicate the traffic dynamics. The network graph is also created based on the network topology by taking vehicles and RSUs as nodes, while establishing links among them based on communication range. This graph is kept dynamically updated depending on vehicle movement in the network. Ultimately, the parameters such as

the communication range, RSU range, vehicle density, simulation time, difficulty of blockchain, and configuration of controllers are set for the simulation process to work well.

3.4. SDN-Based Communication Management

The suggested approach involves the use of centrally managed SDN controller in order to control the communication between the vehicles and the Road Side Units (RSUs) in the IoT-based vehicular network. During the initialization of SDN controller, a complete network knowledge is obtained as the entire network is registered, which includes all vehicles, RSUs, and communication links. The SDN controller continues to monitor the vehicles by collecting the information such as the location of the vehicle, speed of the vehicle, direction of the vehicle, and its communication state.

To improve the connectivity efficiency, the controller implements the mechanism of dynamic allocation of RSUs where each individual car is connected to the nearest RSU. The Euclidean distance between the car and RSU can be defined as:

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (1)$$

where x_i and y_i denote the coordinates of vehicle i , while x_j and y_j represent the coordinates of RSU j . A vehicle is connected to an RSU only when the distance satisfies:

$$d_{ij} \leq R \quad (2)$$

where R is the range of the RSU for communication.

In order to enable the activities for emergency response, the controller prioritizes each car, thereby allowing the emergency cars to be prioritized in communication :

$$p_i = w_1 T_i + w_2 V_i + w_3 D_i \quad (3)$$

where T_i represents the vehicle type, V_i denotes the vehicle speed, D_i is the communication demand, and w_1 , w_2 , and w_3 These are called weights. Depending on these parameters, the controller conducts route management by choosing communication routes with minimal delays and maximum connectivity. Such an SDN based centralized solution increases efficiency in routing, resource utilization and offers reliable communication within the vehicular network.

3.5. Priority-Based Communication

This method of communication is realized by the use of the priority-based communication method to ensure the effective transfer of messages between different types of vehicles. At first, the vehicles are classified into two types, which include the normal vehicles and emergency vehicles including ambulances, fire trucks, and police cars. This sorting helps the SDN controller to differentiate between critical and non-critical traffic. The priority for emergency vehicles is higher than that of other vehicles, ensuring quick connection of the network as well as immediate association with RSUs in an emergency. The SDN controller conducts priority scheduling using the priority level of communication traffic.

This helps to minimize delays in the process and ensures that emergency communication remains continuous. Additionally, resources are dynamically allocated in the form of communication channels, bandwidth, and routes in the network based on the priority of the vehicles and existing network conditions. The combination of these approaches would help to enhance reliable communication in IoT-enabled vehicular networks.

3.6. Blockchain Security Module

The Blockchain Security Module is implemented in the proposed architecture for achieving a secure, transparent, and tamper-proof communication between vehicles, Road Side Units (RSUs), and SDN controller. For each communication process, be it vehicle registration, RSU registration, or data communication, a transaction is generated including the sender ID, receiver ID, timestamp, message details, and hash value of the previous block. Each transaction will be signed digitally to ensure that only legitimate entities of the network perform the communication process. The data of transactions are then hashed using the SHA-256 algorithm to generate a unique hash value:

$$H_i = \text{SHA} - 256(T_i) \quad (4)$$

where T_i represents the transaction data and H_i is the corresponding hash value.

To verify transaction integrity, the computed hash is compared with the received hash:

$$V = \begin{cases} 1, & H_i = H_r \\ 0, & H_i \neq H_r \end{cases} \quad (5)$$

where H_r is the hash received, and V represents the outcome of the validation process.

The valid transaction is incorporated into the new block using the lightweight Proof-of-Work (PoW) consensus algorithm, which determines the value of the nonce so that the hash of the block meets the difficulty criteria for the network:

$$H(B_i \parallel n) < D \quad (6)$$

where B_i is the block data, n is the nonce, and D represents the predefined mining difficulty threshold.

Finally, the generated block is linked to the previous block to construct an immutable blockchain ledger:

$$B_i = \{T_i, H_{i-1}, H_i, n, t\} \quad (7)$$

Where T_i stands for the transactions set, H_{i-1} denotes the hash of the previous block, H_i refers to the current

block's hash, n is the nonce, and t is the timestamp. This chain-based system ensures data integrity, distributed trust, authentication, and tamper-proofing, thus improving the overall security of communication within the proposed IoT-based vehicular network.

3.7. Web Dashboard and REST API

The proposed model consists of a Flask-based web dashboard, which serves as an interactive tool for configuration, control, and monitoring of the vehicular communication network. REST API enables smooth communication between the simulation engine and the dashboard by sending live information about the network state and blockchain transactions. The dashboard allows for real-time monitoring of the vehicle motion, the communications and connection of the RSUs in the simulation. Furthermore, the dashboard offers vehicle visualization, which displays the dynamic position and mobility of the vehicles on the highway. Similarly, blockchain visualization shows transaction information, blocks creation, and ledger state, while controller monitoring shows activities of the SDN controller, network topology updates, RSU distribution, and communications statistics.

3.8. Implementation Environment

Parameter	Specification
Programming Language	Python 3.9
IDE	Visual Studio Code
Framework	Flask
Graph Library	NetworkX
Visualization	Plotly
Blockchain	SHA-256
Consensus	Lightweight Proof-of-Work
API	REST API
Operating System	Windows 11

4. Result and Discussion

The performance analysis of the suggested SDN-blockchain framework for secure intelligent communication in vehicular network based on IoT is discussed in this paper. Simulation outcomes evaluate the performance of dynamic RSU deployment, priority-based communication, routing management, and blockchain transactions processing. The performance of the suggested approach is evaluated through network configurations, communication characteristics, and blockchain-related parameters to show its reliability and security in dynamic vehicular communication environments.

4.1. Performance Analysis of the Proposed Framework

Table 2. Summary of Simulation Performance Parameters

Parameter	Value
Simulation Steps	10
Attached Vehicles	4
Priority Communication Links	3
Active Routes	8
Generated Blocks	6
Pending Transactions	2
Proof-of-Work Difficulty	2

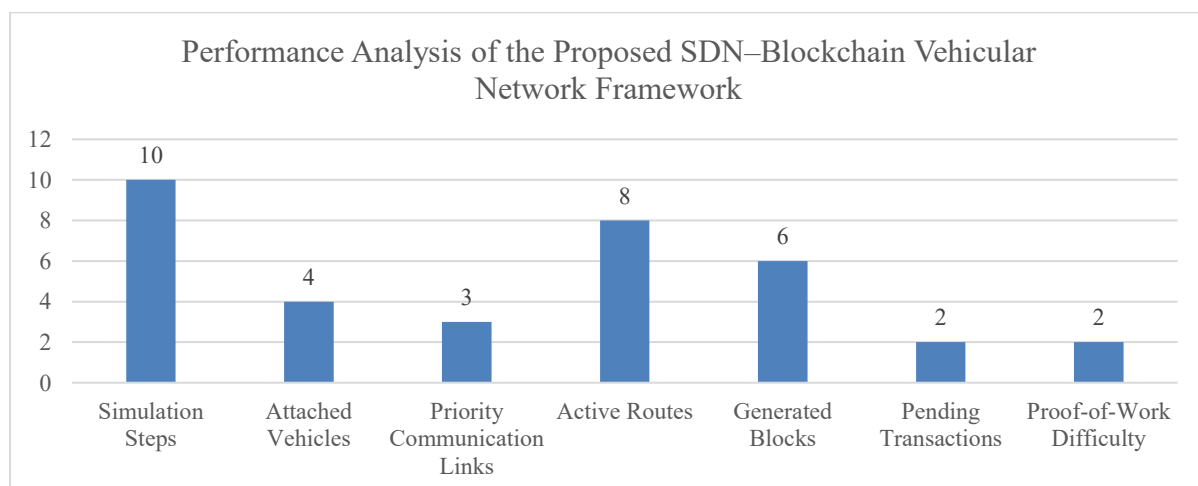


Figure 2. Performance Analysis of the Proposed SDN-Blockchain Vehicular Network Framework

Table 2 and figure 3 shows the performance of the SDN-blockchain framework simulation as a whole. The simulation was able to execute 10 steps while making four vehicle-RSU connections, maintaining three priority communication connections to enable the communication of emergency vehicles. The SDN controller managed to create eight routing connections, showing efficient handling of the network topology and communication processes. Meanwhile, the blockchain component of the design was able to validate and create six blocks, leaving two transactions to be mined during the next round. The proof-of-work difficulty level set to 2 allowed efficient validation of the transactions with low computational effort.

4.2. Vehicle and RSU Configuration Analysis

Table 3. Vehicle and Road Side Unit (RSU) Configuration Parameters

Parameter	Value
Vehicle Priority Level	4
Connected RSUs	1
RSU Communication Coverage	50 m
Maximum RSU Connections	2

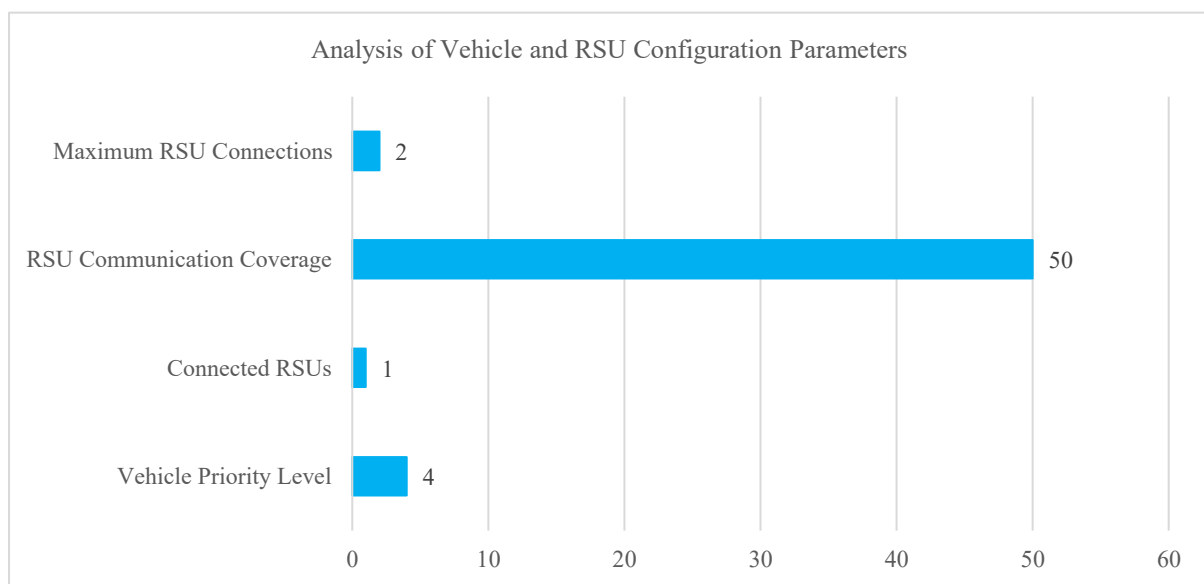


Figure 3. Analysis of Vehicle and RSU Configuration Parameters

Table 3 and figure 3 highlights the values used for configuration parameters for communication between the vehicle and RSU in the suggested framework. The value of 4 for the vehicle priority level ensures priority for emergency vehicles in the communication process. One RSU is used for the communication of each vehicle, whereas the RSU communication range of 50 meters ensures reliable wireless communication in the simulation environment. In addition, each RSU handles a maximum of two vehicle communications at once, ensuring that there is no congestion in the communication process.

4.3. Dashboard Performance Analysis

Table 4. Dashboard Statistics of the Proposed SDN-Enabled Vehicular Network

Simulation Step	Attached Vehicles	Priority Links	Generated Blocks	Blockchain Validity
0	4	3	1	Yes
5	5	3	6	Yes
10	4	3	11	Yes

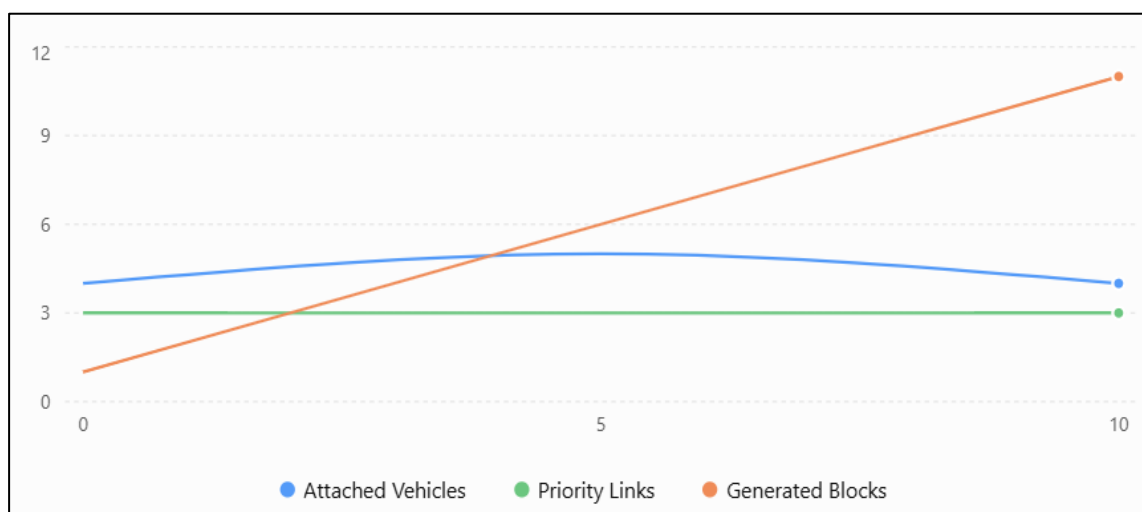


Figure 4. Dashboard Statistics During Simulation

Table 4 and figure 4 represents the dashboard data collected during various stages of the simulation process. The number of attached cars is slightly different due to the mobility of the vehicles, whereas the number of priority communication channels is constant at three to ensure continuous communication of emergency cars. In addition, the blockchain creates a new block continuously, increasing from 1 to 11 through the simulation stage. Moreover, blockchain validation was successful for all simulation stages. This shows the effectiveness of the suggested framework in terms of continuous communication, reliable blockchain process, and monitoring through SDN controller and web dashboard.

4.4. Discussion

The findings from simulations show that the suggested architecture of Software-Defined Networking (SDN) and blockchain has been successful in providing reliable communication, intelligent routing, and secure transaction management in IoT-based vehicular networks. The Software-Defined Networking (SDN) controller successfully conducts RSU allocation and priority-based communication that ensures reliable connection for both normal and emergency vehicles. At the same time, the blockchain module successfully creates secure and tamper-proof transaction records by creating blocks. The simulation research has some limitations as well. It has been conducted in a simulated environment and with a rather small number of nodes in a network and the centralized SDN controller. Moreover, the Proof-of-Work (PoW) consensus used in the research might generate extra load in more complex environments.

5. Conclusion

This study investigated how the integration of Software-Defined Networking (SDN) and blockchain technology can improve secure, intelligent, and reliable communication in IoT-enabled vehicular networks. The proposed framework demonstrated that centralized SDN control enables efficient dynamic RSU allocation, adaptive routing, and priority-based communication for emergency vehicles, while blockchain ensures secure transaction validation, data integrity, and decentralized trust. These capabilities contribute to enhanced network performance, reduced communication delays, and improved resource utilization, making the framework suitable for next-generation intelligent transportation systems. Although the simulation results are promising, the study is limited by its simulation-based evaluation, relatively small network scale, and the use of a lightweight Proof-of-Work consensus mechanism, which may affect scalability in large deployments. Future research should focus on real-world implementation, distributed SDN.

References

- [1] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart Transportation: An Overview of Technologies and Applications," 2023. doi: 10.3390/s23083880.
- [2] H. Yan and Y. Li, "Generative AI for Intelligent Transportation Systems: Road Transportation Perspective," *ACM Comput. Surv.*, vol. 57, no. 12, pp. 1–45, Jul. 2025, doi: 10.1145/3719290.
- [3] M. L. Tumminello, E. Macioszek, and A. Granà, "Emerging Cutting-Edge Technologies and Applications for Safer, Sustainable, and Intelligent Road Systems in Smart Cities: A Review," Nov. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/app15211583.
- [4] A. V. Jha, B. Appasani, M. S. Khan, S. Zeadally, and I. Katib, "6G for intelligent transportation systems: standards, technologies, and challenges," *Telecommun. Syst.*, vol. 86, no. 2, pp. 241–268, Jun. 2024, doi: 10.1007/s11235-024-01126-5.
- [5] T. Yuan, W. Da Rocha Neto, C. E. Rothenberg, K. Obraczka, C. Barakat, and T. Turetletti, "Machine learning for next-generation intelligent transportation systems: A survey," *Trans. Emerg. Telecommun. Technol.*,

- vol. 33, no. 4, Apr. 2022, doi: 10.1002/ett.4427.
- [6] F. A. Butt, J. N. Chattha, J. Ahmad, M. U. Zia, M. Rizwan, and I. H. Naqvi, "On the Integration of Enabling Wireless Technologies and Sensor Fusion for Next-Generation Connected and Autonomous Vehicles," *IEEE Access*, vol. 10, pp. 14643–14668, 2022, doi: 10.1109/ACCESS.2022.3145972.
- [7] M. Sadaf *et al.*, "Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects," 2023. doi: 10.3390/technologies11050117.
- [8] X. Mu and M. F. Antwi-Afari, "The applications of Internet of Things (IoT) in industrial management: a science mapping review," 2024, *Taylor and Francis Ltd.* doi: 10.1080/00207543.2023.2290229.
- [9] Y. Rajkumar and S. V. N. Santhosh Kumar, "A comprehensive survey on communication techniques for the realization of intelligent transportation systems in IoT based smart cities," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 3, pp. 1263–1308, May 2024, doi: 10.1007/s12083-024-01627-9.
- [10] C. Fu, B. Wang, and W. Wang, "Software-Defined Wide Area Networks (SD-WANs): A Survey," 2024. doi: 10.3390/electronics13153011.
- [11] M. El-Hajj, "Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions," 2025. doi: 10.3390/network5010001.
- [12] M. Malakar, J. Mahapatro, and T. Ghosh, "A survey on routing and load-balancing mechanisms in software-defined vehicular networks," *Wirel. Networks*, vol. 30, no. 5, pp. 3181–3197, Jul. 2024, doi: 10.1007/s11276-024-03729-x.
- [13] S. Hussain, S. Tahir, A. Masood, and H. Tahir, "Blockchain-Enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV)," *IEEE Access*, vol. 12, pp. 110992–111006, 2024, doi: 10.1109/ACCESS.2024.3431279.
- [14] Z. Ma *et al.*, "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," *IEEE Access*, vol. 12, pp. 81471–81482, 2024, doi: 10.1109/ACCESS.2024.3409361.
- [15] N. Hameed Hussein *et al.*, "SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges," *IEEE Access*, vol. 13, pp. 126801–126861, 2025, doi: 10.1109/ACCESS.2024.3355313.
- [16] S. Aizaz Ul Haq, M. Imran, N. Shah, and G. M. Muntean, "SDN-Based Edge Computing in Vehicular Communication Networks: A Survey of Existing Approaches," *IEEE Access*, vol. 13, pp. 74252–74287, 2025, doi: 10.1109/ACCESS.2025.3561083.
- [17] S. Dwivedi, R. Amin, A. Das, M. Leung, K. C.-A. H. Networks, and U. 2022, "Blockchain-based vehicular ad-hoc networks: A comprehensive survey," *ElsevierSK Dwivedi, R Amin. AK Das, MT Leung, KKR Choo, S VollalaAd Hoc Networks, 2022•Elsevier*, vol. 137, pp. 1–26, 2022, Accessed: Jul. 14, 2026. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1570870522001536>
- [18] I. M. Varma and N. Kumar, "A comprehensive survey on SDN and blockchain-based secure vehicular networks," 2023. doi: 10.1016/j.vehcom.2023.100663.
- [19] G. N. Nurkahfi *et al.*, "On SDN to Support the IEEE 802.11 and C-V2X-Based Vehicular Communications Use-Cases and Performance: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 95926–95958, 2024, doi: 10.1109/ACCESS.2023.3341092.
- [20] R. Sarpong, F. Araújo, and B. Sousa, "The potential of SDNs and multihoming in VANETs: A Comprehensive Survey," in *Proceedings - 2025 12th International Conference on Future Internet of Things and Cloud, FiCloud 2025*, 2025, pp. 265–272. doi: 10.1109/FiCloud66139.2025.00043.
- [21] R. Almutairi, G. Bergami, and G. Morgan, "Systematic Literature Review of VANET Simulators: Comparative Analysis, Technological Advancements, and Research Challenges," in *Proceedings of the 1st International Symposium on Parallel Computing and Distributed Systems, PCDS 2024*, 2024. doi: 10.1109/PCDS61776.2024.10743218.