Intelligent Multimedia Processing & Communication Systems Journal

IMPCSJ

J IMPCS (2025) 21: 47-57
DOI 10.71856/IMPCS.2025.1221085

Research Paper

Secure Separation of the Infrastructure in Software-defined Overlay-enabled Internet of Vehicles (IoV)

Shahram Bahrak[1], Mani Zarei[2*]

1. MSc, Department of Computer Engineering, ShQ.C., Islamic Azad University, Shahr-e Qods, Iran, Shahram.bahrak@iau.ir
2. Assistant Professor, Department of Computer Engineering, ShQ.C., Islamic Azad University, Shahr-e Qods, Iran,
* *Corresponding Author*, mani.zarei@iau.ac.ir

Article Info

Article history:
Received: 2 Aug 2025
Accepted: 13 Sep 2025

Keywords:
Internet of Vehicles (IoV),
Overlay model,
Software-defined networking.

ABSTRACT

The Internet of Vehicles (IoV) is becoming increasingly popular in both academic communities and modern industrial ecosystems. The shared communication substrate of IoV networks with other communication networks, such as mobile networks and mobile data networks, can impose significant security risks on neglecting security upgrading of this infrastructure and the absence of a proper policy for selecting the key elements of the network can readily disrupt the Intelligent transportation system (ITS). Software-defined networking (SDN), with ITS intrinsic capabilities, can render IoV networks more secure and scalable. SDN provides advantages such as improved traffic control, smart routing, quality of service, and road-aware decision making. One effective SDN approach is to employ a coverage model. The overlay model enables the creation of a virtual network consisting of authorized nodes atop the physical network to realize the decoupling of the physical layer, which can be regarded as the first line of defense for network security. In this paper, an SDN overlay model for the IoV is proposed to enable a secure communication infrastructure. The model consists of establishing a virtual and geographically partitioned network over the underlying physical network, along with the creation of communication tunnels and encryption of information packets, thereby forming a multi-path mesh connectivity. Simulation results show that the proposed model can improve end-to-end delay, resource utilization, and average response times compared to both other SDN networking approaches and traditional models. The proposed model creates a suitable roadmap for improving security concerns in this field.

I. Introduction

The Internet of vehicles (IoV) has recently attracted significant attention in both academic and industrial communities, with various applications aimed at improving road safety and comfort [1]. Delay-sensitive safety applications require multi-path route planning to select optimal paths with minimum latency. Geographic partitioning and division of a large network into smaller subnetworks can reduce broadcast and multicast traffic [2]. Mobility and vehicular displacement are among the primary challenges of IoV networks, causing abrupt changes in network connectivity and presenting numerous routing challenges. Routing rules in these networks must mitigate congestion and traffic on network links.

Given the high sensitivity to delay in automotive networks, all network requirements should be addressed such that computational and networking needs are met rapidly. This motivates the use of mobile edge computing vehicles and fixed edge computing nodes (i.e., static roadway infrastructures) to provide computational services concurrently [3]. The advantages of software-defined networking (SDN) networks have led these networks to come to the aid of vehicular Internet networks and create networks with higher capabilities. Capabilities such as traffic engineering, traffic-aware routing, and quality of service are all advantages of these networks. Also, having a powerful controller and separating the control plane from the data plane enables centralized, holistic, and traffic-aware routing decisions. This can reduce latency, enable alternative paths, and continuously monitor link quality.

Future networks must be resilient to dynamic topology and intra-network communications and meet growing expectations for adaptability [4]. Security is a fundamental requirement of communication networks, and in IoV. This concern is even more critical. Isolating vehicular networks from mobile and mobile-data networks sharing a common communication substrate constitutes a first step toward security, ensuring that all nodes joining the network possess the necessary permissions. Physical-layer isolation of IoV infrastructures from other networks sharing the same substrate can further enhance security.

Many IoV network models using long-term evolution (LTE) and SDN have been proposed, but they have struggled to realize effective isolation of heterogeneous networks operating on cellular substrates. Implementing SDN in an overlay fashion and creating virtual tunnels between network zones can enhance communication security, improve scalability, and reduce broadcast multicast traffic, thereby addressing local needs with lower delay.

Emerging technologies for IoV networks have been proposed to improve performance. Since IoV networks depend on diverse communications such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P), they are susceptible to multiple security threats

Emerging technologies have been developed to enhance the performance of IoV networks. Given that IoV networks rely on diverse communications such as V2V, V2I, and V2P, they are susceptible to multiple security threats that may disrupt information flow and lead to significant consequences. Malicious vehicles in IoV networks can launch various attacks, including man-in-the-middle (MITM), Denial of Service (DoS), eavesdropping, identity spoofing, replay attacks, and more. MITM attacks may provide misleading information about road signs or road conditions [5]. Inadequate measures, weak encryption, and privacy concerns may expose critical data such as vehicle location, speed, and driver identity. Eavesdropping can lead to exposure of driver profiles. Moreover, identity spoofing and MITM attacks may enable unauthorized control over vehicle operations. Ensuring the integrity and reliability of data for real-time critical decision-making is essential. Additionally, replay attacks can cause delays in emergency responses by presenting erroneous data. The unique characteristics of IoV, namely, dynamic behavior, give rise to security challenges that traditional security solutions cannot adequately address [6].

The contributions of this paper are summarized below:

- Creating a virtual network atop the underlying infrastructure to form an IoV network with real nodes, effectively serving as the primary security layer of the network.
- Partitioning based on geographical location and assigning distinct IP addresses to each zone to reduce network traffic, especially broadcast/multicast traffic.
- Establishing communication tunnels between zones, along with encryption of data packets, to form multi-path mesh connectivity, reduces transport delay, preventing data loss, and achieving high scalability.
- The model is fully simulated on the EVE-NG simulator, and all reported results are derived from this model.

The remainder of the paper is organized as follows. Section II presents the background of the research and past work, and Section III describes the proposed methods and models. Section IV presents an evaluation and comparison of the proposed architecture, including comparative diagrams, evaluation metrics, and related explanations. Finally, Section V provides the conclusions and future work.

II. Related Works

Muhana Magboul and Ali Muslam [7] discuss the emergence of V2V communications, which has brought substantial advancements and opportunities to the

automotive innovations industry. The exchange of information among vehicles has the potential to transform road safety, traffic control, and overall transportation efficiency. Nevertheless, safeguarding the transmission and protection of data in V2V communications is crucial to maintaining the integrity, privacy, and reliability of the shared information. With the broad adoption of vehicle-to-everything (V2X) communications, security and privacy assurances become a fundamental concern. A proposed solution is a multi-protocol gateway to facilitate efficient exchange.

Yingxun Wang [8] notes that ICT and artificial intelligence have driven a rapid increase in the number of IoT-enabled devices for over two decades [9]. According to statistics, the number of IoT-connected devices is expected to reach nearly 40 billion by the end of 2030 [10]. IoV is one of the primary IoT applications, often described as the "IoT on wheels," emerging from the convergence of traditional vehicular ad hoc networks with IoT. In the IoV ecosystem, each vehicle is regarded as a smart Internet-enabled entity equipped with a powerful multi-sensor platform, computing unit, communications technologies, and IP-based Internet connectivity for sensing, processing, and communications. Additionally, V2X communications facilitate seamless connectivity among entities within an IoV network to realize the various automotive applications [11]. If a particular vehicle within an IoV network becomes the target of a malicious attack, a substantial risk to the entire IoV network arises. Consequently, multiple solutions have been proposed by researchers in academia and industry; among them, cryptography is arguably the most prominent to address these concerns effectively.

Debashis et al. [12] present a blockchain-based smart IoV framework, BSIoV. Blockchain can enhance characteristics such as collaboration, transparency, and security in automotive networks, enabling secure and transparent vehicle-to-everything communications among regulators and industry stakeholders to facilitate trustworthy vehicle communications with other entities. Debasis et al. and colleagues [12] present a blockchain-based smart IoV framework, BSIoV, wherein blockchain can enhance collaboration, transparency, and security within vehicular networks, enabling secure and transparent V2X communications with other entities.

Mohammad Shahzad and colleagues [13] discuss a large-scale SDN paradigm for on-demand resource utilization, which is expected to play a pivotal role in the future of the IoT. Their approach emphasizes a versatile and scalable network framework that can adapt to the rapid growth of devices and IoT applications. The combination of static mapping and dynamic traffic flow distribution over time and space creates load imbalances across SDN controllers. Dynamic mobility is proposed as a solution to rebalance the load by redistributing traffic among SDN controllers.

E.Khezri et al. [14] introduce a multi-layer model that employs parked vehicles to realize multi-path routing over SDN networks. Incorporating multi-path routing reduces end-to-end routing latency, lowers bandwidth consumption, and enhances link stability. The group investigates creating multiple alternate multi-path routes by leveraging parked vehicles.

SR.Pokhrel [15] identifies three core challenges in vehicular networks: network scalability, security, and quality-of-experience (QoE) flexibility. By utilizing SDN-based architectures and implementing a set of security policies, the proposed model aims to provide a scalable and secure vehicular network. The model relies on Wi-Fi connectivity and TCP-based simulations, inspired by federated learning approaches, to estimate QoE requirements and to mitigate heterogeneity across nodes, contributing to more robust and adaptable deployments.

A.Akbar et al [16] propose SEAC, a vehicular social network (VSN) approach that integrates clustering techniques with SDN. This three-dimensional modeling framework builds logical clusters based on physical location, social ties, and shared interests among vehicles. In this model, vehicles can form independent social relationships to create an overlay social network that facilitates information exchange.

M.T.Abbas et al [17] introduce the concept of an edge controller as the operational backbone of the vehicular network. The aim is to ensure optimal and durable shortest paths while maintaining connectivity. By leveraging cellular connectivity and transmitting SDN control messages over these links, they achieve minimized network latency and reduced traffic.

Ho et al. [1] demonstrate simultaneous involvement of static and mobile nodes with SDN-enabled networks to substantially reduce computation latency in vehicular networks. The authors argue that the stability of vehicular network connections is imperfect, thereby necessitating the use of reliable nodes to perform tasks and meet application deadlines.

D.T.Nguyen et al. [18] propose a practical model for dynamic offloading of applications on mobile edge nodes (MENs) enabled by SDN Networking. The objective of this model is to achieve optimal offloading of computational load and to assist in finding offloading paths while providing bandwidth guarantees through SDN technology. A primary challenge of mobile edge computing systems is achieving efficient collaboration and coordination among MENs so that all nodes participate in the available computations (i.e., avoiding idle nodes or overwhelmed nodes). For example, when the computational capacity of a node reaches the Intelligent Transportation System (ITS) limit, the offloaded computations can be forwarded to a neighboring MEN rather than to the cloud.

A.J.Kadhim et al. [19] present an SDN-based model aimed at enabling delay-sensitive tasks to execute within prescribed time bounds. By clustering the network and placing a load balancer that acts as a local controller, the approach seeks to maximize the utilization of local processing and networking resources, thereby minimizing the need for cloud servers that introduce additional latency.

B.Alaya et al. [20] develop a hybrid architecture and propose a dynamic approach to optimize the placement of controllers, along with services for topology estimation based on machine learning techniques. It also introduces a secure and intelligent scheme for receiving and securely sharing messages, to achieve a flawless (fault-tolerant) vehicular network architecture to support ITS services.

As you can see, none of the models created have done any serious and fundamental work on network infrastructure security, which is definitely the first and perhaps the most important part in creating security. Also, creating a virtual network with authorized nodes can play an important role in the scalability of the created network. The presented model has been able to improve the security of IoV networks by separating the network infrastructure and also creating a segmented virtual network.

III. Methodology

separating the physical substrate IoV networks from other networks that share the same infrastructure can constitute an initial step toward enhancing the security of these networks. On the one hand, partitioning IoV can improve its scalability **[21]**, which in turn reduces broadcast and multicast traffic within IoV networks. The outcome of this reduction is an improvement in the scalability of the networks and a decrease in the latency of performing computations.

Given the numerous challenges associated with routing in the IoV network due to abrupt topology changes, traditional routing approaches based on static neighborhood discovery methods cannot adequately meet the requirements of these networks and may exacerbate network latency [22, 23]

Physical-layer separation implies that mobile networks, mobile data networks, and the IoV can be decoupled by constructing a virtual network using SDN Networking. This approach reduces the overhead involved in separating IoV network infrastructures and eliminates the need to employ traffic-tagging methods for traffic separation among networks sharing the same underlying infrastructure.

Furthermore, employing an SDN networking overlay model leads to the creation of virtual communication tunnels, which play a critical role in encryption and in establishing full-graph connectivity between two connectivity zones. These tunnels yield pre-defined alternate paths that can be beneficial in critical situations (e.g., active link failure, degraded quality of service, or bandwidth saturation).

In this architecture, the data plane is decoupled from the control plane; data transmission decisions are not made inside the hardware in real time but are aggregated either in a centralized hardware component or implemented in software. In fact, the SDN controller is the sole element that can intervene in data forwarding, and all network devices are managed under the SDN controller.

System Architecture

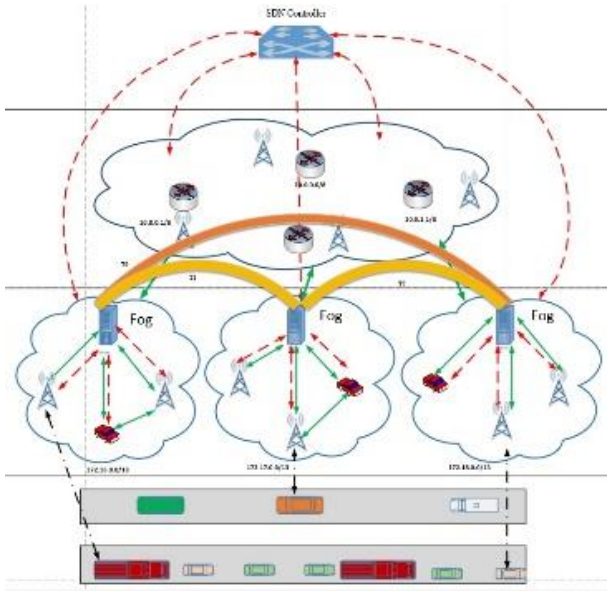
In this section, the topology of the network model for our IoV networks is first discussed, and the aspects that require careful consideration are highlighted.

Next, the role of the orchestration component for software-defined networks is discussed.

In the third section, the mechanism for creating a virtual network and establishing communication tunnels is described.

Subsequently, the design of the underlying IP address structure and the created zones is addressed.

Finally, the proposed model's routing methodology is discussed.



A. Network Topology

If this model were deployed in a city like Tehran, the city would be divided into different zones based on ITS infrastructure and traffic patterns (see Figure 1). Each zone

Figure 1: Overall IoV Network Infrastructure Topology and Overlay Virtual Network

would have one or two gateways that connect it to outside networks. These gateways need to be placed where the telecommunications system is strongest, for example, at fiber-optic backbone sites. These locations are usually linked to each other in a full-mesh network.

Because resource management in SDN networking SDN-enabled networks is governed by the network controllers, discovering infrastructural and computational resources (i.e., urban facilities) and delegating their management to the SDN controller is essential and critical. Enhancement and establishment of augmentation links, as well as leveraging existing computational resources (e.g., parked vehicles, static vehicles in parking lots, and other idle resources in the city), are considered exemplars of this category.

Utilizing multiple frequency bands for gateway nodes can be beneficial [24] to create augmentation links. In the proposed modeling, we attempt to exploit urban resources,

such as those available in Tehran, for this purpose. Since some base transceiver stations (BTS) are interconnected via city-provided high-speed and reliable fiber-optic facilities, while others are connected via microwave links, we model each node with two communication interfaces: (i) a fiber/cable-based connection and (ii) a microwave/wireless link. These dual connections play a key role in establishing reliable and persistent connectivity with network elements under the main SDN controller.

Operating with dual active-active connections is a core requirement for SDN-enabled networks to mitigate threats such as link failure, link congestion, degraded quality of service, and related issues. Moreover, the two connections can be employed simultaneously to maintain inter-zone connectivity.

To satisfy the computational resource demand of each zone, local resources within the same zone can be used. Such resources may include the number of operational servers at the network edge of the zone, pools of parked vehicles in a given parking facility, or any other idle resources within that zone.

The topology of vehicular networks is highly dynamic and largely unpredictable. To mitigate the adverse effects of such changes, certain elements are designated as stationary computational and network resources, which do not move, while moving vehicles are treated as clients of the network. This approach reduces the rate of topology changes and alleviates the operational burden on the network controller.

B. Coordinator Role in IoV Networks

SDN networks offer additional advantages, including network customization, rapid topology changes, reduced capital expenditure, and more. However, deploying SDN-based networks also entails risks that must be identified and mitigated. The separation of the data plane and the control plane, while providing many benefits, also presents implementation challenges: in SDN architectures, the data plane and the control plane must be brought into coordination without introducing delays, noise, or other detrimental effects. The coordination between these planes is performed by a coordinator.

The coordinator establishes a temporary, on-demand, encrypted connection with the controller and with network elements that act as service-nodes and form the backbone of the network. After mutual authentication of the nodes, the coordinator registers them with the network controller. Following this, the controller advertises the

infrastructure address (underlying network) and the local addresses of networks connected to the infrastructure to the gateway nodes. From that point on, each vehicle seeking connectivity can access local services via local addresses and remote services via remote addresses after a tunnel has been established.

C. Virtual Network Creation

Following the establishment of adjacency between network hardware and the SDN controller, the gateway of each zone transmits ITS network information to the SDN controller after authentication by the network controller. After information exchange between the SDN controller and the edge devices in each zone (i.e., gateway of each zone), a tunnel is established for every link between the two sides, and these two tunnels are used for transmitting the control data of each zone. Using these two tunnels, each zone sends ITS information, IP address, underlying infrastructure address, and operational IP of the zone to the SDN controller. With the first connectivity request between two zones, tunneling for that connection is established, and these tunnels remain persistent for as long as the underlying infrastructure is active. Since these tunnels are created using the IPsec protocol, the communication is secure, and due to the full-mesh connectivity between zones, network accessibility is enhanced.

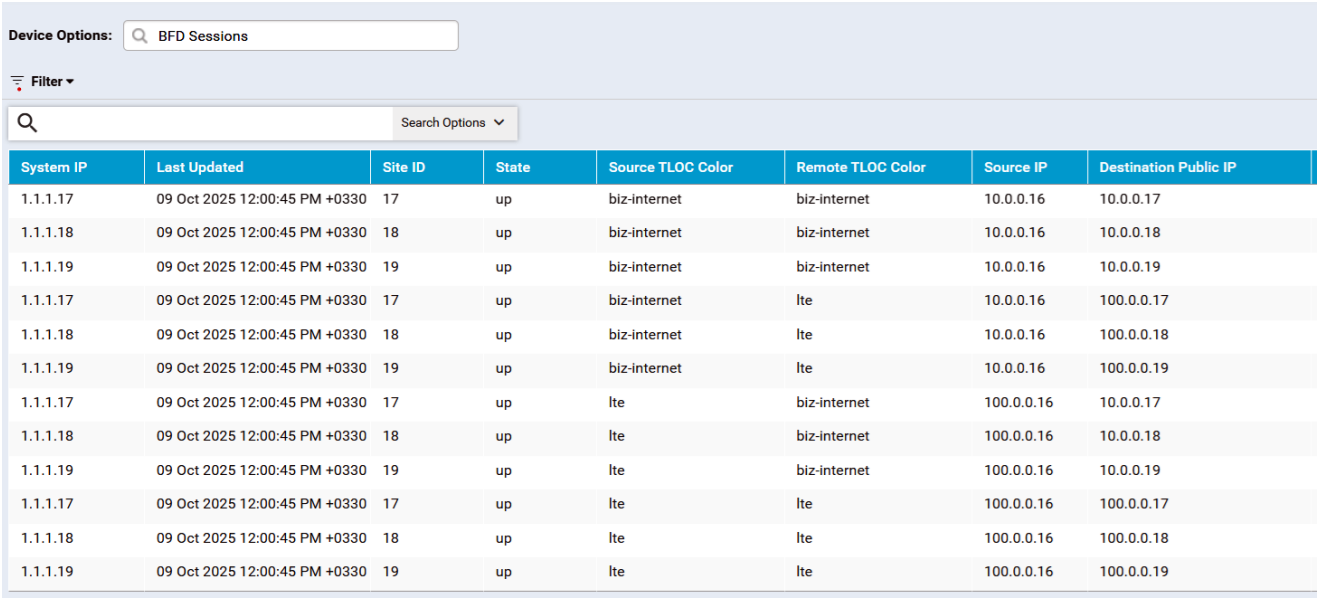
Security Policy Creation and Enhanced Availability

By implementing targeted policies, network connectivity can be adapted to meet requirements, and a more complete full-mesh connectivity can be created. This leads to reduced latency and higher availability of services across the network.

Figure 2, which is extracted directly from the simulator controller used, shows the superiority of the proposed model, which, for every two active links between two districts, there will be four tunnels, creating a total of 12 tunnels.

These tunnels play a key role in availability, traffic distribution, and bandwidth management. Extending the network to M zones and N infrastructure links, per zone, results in $(M-1).\ N^2$tunnels.

This expansion drives benefits such as enhanced connectivity, higher availability, improved bandwidth management, confidentiality of transmitted data, and greater data integrity. All of these factors contribute to a stronger realization of security attributes aligned with the CIA triad (Confidentiality, Integrity, Availability).



System IP	Last Updated	Site ID	State	Source TLOC Color	Remote TLOC Color	Source IP	Destination Public IP
1.1.1.17	09 Oct 2025 12:00:45 PM +0330	17	up	biz-internet	biz-internet	10.0.0.16	10.0.0.17
1.1.1.18	09 Oct 2025 12:00:45 PM +0330	18	up	biz-internet	biz-internet	10.0.0.16	10.0.0.18
1.1.1.19	09 Oct 2025 12:00:45 PM +0330	19	up	biz-internet	biz-internet	10.0.0.16	10.0.0.19
1.1.1.17	09 Oct 2025 12:00:45 PM +0330	17	up	biz-internet	lte	10.0.0.16	100.0.0.17
1.1.1.18	09 Oct 2025 12:00:45 PM +0330	18	up	biz-internet	lte	10.0.0.16	100.0.0.18
1.1.1.19	09 Oct 2025 12:00:45 PM +0330	19	up	biz-internet	lte	10.0.0.16	100.0.0.19
1.1.1.17	09 Oct 2025 12:00:45 PM +0330	17	up	lte	biz-internet	100.0.0.16	10.0.0.17
1.1.1.18	09 Oct 2025 12:00:45 PM +0330	18	up	lte	biz-internet	100.0.0.16	10.0.0.18
1.1.1.19	09 Oct 2025 12:00:45 PM +0330	19	up	lte	biz-internet	100.0.0.16	10.0.0.19
1.1.1.17	09 Oct 2025 12:00:45 PM +0330	17	up	lte	lte	100.0.0.16	100.0.0.17
1.1.1.18	09 Oct 2025 12:00:45 PM +0330	18	up	lte	lte	100.0.0.16	100.0.0.18
1.1.1.19	09 Oct 2025 12:00:45 PM +0330	19	up	lte	lte	100.0.0.16	100.0.0.19

Fig. 2. Outputs produced by the SDN controller and the generated virtual tunnels

Infrastructure Security

Creating a virtual network atop the physical infrastructure isolates nodes and hardware that share the same underlying infrastructure but serve different use cases. In other words, we maintain a fixed infrastructure with multiple, distinct networks, and this separation enhances the physical-layer security, which is the first line of defense in security. Another benefit of virtual network creation is the zoning of a large network into smaller zones, which reduces broadcast traffic and, in turn, improves security and access management through segmentation.

IP PLAN

Two independent IP address ranges are defined for the network. The first range is reserved for the infrastructure (underlying network), designated as 10.0.0.0/8, and the second range is allocated for the vehicles participating in the IoV network, designated as 172.16.0.0/13.

Table 1 shows the zone number and IP address of each zone.

TABLE I: IP address allocation to zones and network segments

Ip address	Area Number
172.16.0.0/13	Area1
172.17.0.0/13	Area2
172.18.0.0/13	Area3
172.19.0.0/13	Area4
172.20.0.0/13	Area5
172.21.0.0/13	Area6
172.22.0.0/13	Area7
172.23.0.0/13	Area8

Routing

In the proposed model, an overlay-based method is used to deploy the SDN IoV network. This method creates virtual tunnels between different zones, establishing a full mesh network among the zones, and then advertising the virtual network addresses within each zone.

The operation proceeds as follows: initially, all infrastructure nodes and elements (RSUs, edge-network nodes, fixed vehicles, and other components) are connected to the network controller via cellular communications and optical fiber. This underlying network is maintained as a permanent and always-available infrastructure. Network clients never use this infrastructure directly for inter-zone or intra-zone communications. In our simulator, the IP address of this underlying infrastructure network is assumed to be 10.0.0.0/8.

To enable intra-zone and inter-zone communications, a virtual network is employed. The SDN controller knows all infrastructure elements, the IP addresses of the virtual network, and the routes to reach them.

If a vehicle wishes to communicate with another vehicle within a specific zone, the communication is straightforward because both vehicles reside in the same zone and share a common IP address range.

If two vehicles are in different zones, the request is first sent to the gateway of the originating zone. The gateway then forwards the address of the destination zone to the central controller. In response, the central controller provides the underlying infrastructure address of the destination zone (destination IP address, gateway, etc.) to the gateway of the first zone. Then, a communication tunnel is established by the gateway of Zone 1 with its own IP address as the source and the IP address of the destination zone gateway as the destination. From that point onward, all communications between Zone 1 and Zone 2 are carried out over this tunnel.

Notes for IEEE-style refinement (optional, if you want full formal formatting): Terminology consistency: Road-Side Unit (RSU), SDN controller, virtual network, and zone gateways.

The 10.0.0.0/8 addressing plan can be presented in a dedicated subsection as part of the infrastructure addressing. Consider defining intra-zone vs. inter-zone communications, tunnel setup procedures, and security considerations in subsequent sections.

The tunnels created between the gateway nodes of each network, which are intended to serve as gateways in their respective zones, are established. As previously stated, these gateway nodes act as the backbone of the network and use high-speed connections with fiber-optic augmentation. In fact, we implement SDN at network points where the Connections are not undergoing drastic changes and where the backbone role is present. This approach reduces overhead and the burden on the SDN controller.

For example, if IP 10.0.0.1 and 10.0.1.1 are the edge (gateway) addresses of zone 1 and zone 2, and 172.16.0.0\13 and 172.17.0.0\13 are the virtual networks of zone 1 and zone 2, respectively, and a connection between zone 1 and zone 2 is desired, the tunnel created will be scoped to the source and destination addresses. In other words, the SDN controller informs the gateway nodes how to form the tunnel IPs for connectivity to each zone.

Tunnels can be established in two forms: Generic Routing Encapsulation (GRE) and GRE over IPsec. Depending on the requirements and latency constraints, one of them can be selected. If security is a priority, GRE over IPsec is recommended.

The delay in establishing the tunnel is minimal because the SDN controller holds all the necessary Information to connect to the edge routers of each zone. Moreover, after the tunnel is established, the SDN controller is responsible for session maintenance.

By registering and classifying vehicle IPs within each zone according to their usage, we can exert finer control over zone-specific requests. Consider a scenario in zone 1 of the city where a traffic accident occurs. The accident vehicle may request the presence of police, fire brigade, or ambulance, either from the local zone or from other zones. Assuming a reserved IP allocation tied to physical location and application, requests can be routed to a specific zone and to certain IPs rather than broadcasting across the entire network. This enhances scalability and reduces network traffic, enabling local servicing of most requests. Specifically, an accident vehicle would first receive assistance from the local ambulance, police, and fire brigade, and then from other zone l entities as needed.

In practice, requests can be served in two ways: locally with a multi-packet (multi-hop) delivery approach, and, if no local response is available, in a broader, public manner via tunnels that connect different zones.

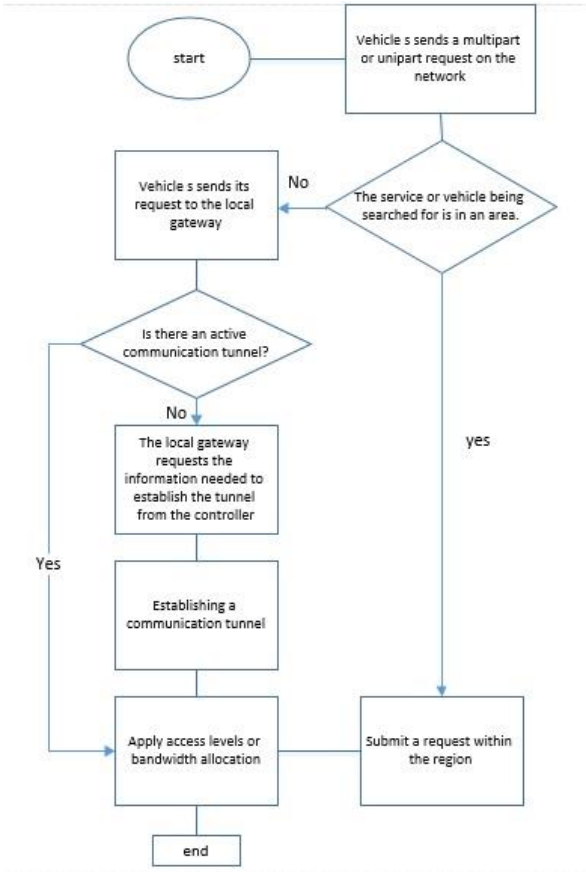


Fig. 3. Flow Chart of Handling Local and Non-local Requests

In the proposed model, all vehicles in the network must obtain the necessary licenses and permissions from the competent authorities to be recognized as trusted nodes within the network. Subsequently, all hardware components present in the network, such as RSUs and base stations (BSs), are introduced to the SDN controller. This operation is performed by the network orchestrator.

By tracking the daily mobility paths of vehicles and recording them over 24 hours, diverse policies can be implemented.

The initial selection of vehicles and the creation of a virtual network on the underlying infrastructure ensure that other network nodes that rely on cellular connectivity, such as mobile devices and mobile Internet users, are not part of the virtual network. This approach ensures that only trusted nodes participate in the virtual network, leading to a significant enhancement of the underlying network security.

Additionally, network segmentation and the establishment of direct inter-zone connectivity via the network controller contribute to the scalability of the proposed architecture. A secondary advantage of segmentation is the reduction of broadcast and multipoint traffic across the network.

Consider a scenario where a traffic accident occurs and information about the incident is to be transmitted to the nearest police vehicle, fire brigade, and ambulance. The request is disseminated by the accident vehicle to all nearby police, fire brigade, and ambulance units, and the nearest responsive vehicle will provide the appropriate reply.

Another advantage of network segmentation is that local requests and needs can be served locally. The establishment of tunnels and on-demand connections enhances security at the network layer because, firstly, the network traffic is re-encapsulated and encrypted; secondly, the possibilities of data tampering or eavesdropping are mitigated. Figure 3 illustrates the steps in this process.

An additional benefit of employing SDN is the separation of control information from data traffic, which allows control-plane traffic to be given priority in transmission.

The SDN controller continuously tests connectivity and the quality of links to constantly strive for the best routing decisions. This is performed by periodically sending control packets (e.g., hello packets) and by measuring the round-trip time of these probes to compute the delay of each connection, which informs subsequent decision-making.

The computation of the delay for each connection and the allocation of the required resources for each service ensure that bandwidth constraints are respected when selecting a path.

Moreover, global network policies can be defined by specifying multiple roles. These policies fall into two categories: control policies, which influence the overall network behavior, and data policies, which affect the prioritization of communications and access levels.

IV. Performance Evaluation

In this chapter, the statistical analysis of the study is presented. The approach consists of independently simulating all three models first, followed by a comparison of their outputs in the form of charts. These three methods are selected to demonstrate the impact of SDN networking overlay technologies on the IoV network.

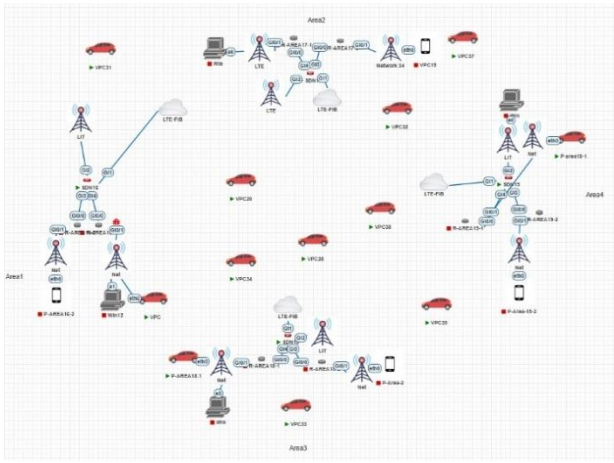
- Model 1, referred to as SDN-L, represents the IoV network that does not employ SDN; routing is implemented based on existing and proposed algorithms without SDN.
- Model 2, referred to as SDN-M, is based on SDN and utilizes the default settings of the SDN controller.
- Finally, Model 3, referred to as SDN-MP, aims, in addition to leveraging SDN networks, to apply policies given the understanding of the available service and the required capabilities for deploying services that improve the network's requirements.

Simulation Requirement

The proposed model is an SDN-based IoV overlay network which benefit from virtual tunnels to design extension communications and encrypt transmitted data. Since the implementation of the intervehicle tunneling in existing automotive simulator environments and customized frameworks, including OMNeT ++, NS3, VEINS, etc., is inherently impossible, the EVE-NG simulator is used to create a virtual network and support communication tunnels in IoV ecosystem. In addition, Cisco controllers are used in SDN WAN networks to apply management policies and reconfiguration capability.

Vehicles in the proposed model are client nodes, and the SDN requirement is implemented on the network infrastructure and the service hosts in the IoV network backbone. All evaluations and comparisons are implemented on the network backbone correspondingly, and inter-vehicle communications are inherently ineffective in performance evaluation of the proposed model.

This choice enables proper implementation of both the network Controller and the tunnel communications of the model. Figure 4 shows the topology of the model designed in the eve-ng environment.



123

Fig. 4. Simulated topology of the proposed model on the EVE-NG simulator

For network monitoring, network monitoring tools such as OpManager software, PingPlotter5, and Zabbix software were employed to extract more reliable outputs.

To enable overlay-based comparison and simulation of SDN networks, a controller capable of creating a virtual overlay network is required. In this simulation, Cisco controllers were used. This controller utilizes an overlay protocol called OMP, which is a TCP-based comprehensive protocol that builds Cisco's overlay control plane across wide-area networks.

Simulation Parameters

To accurately evaluate the proposed model and in light of the factors identified in the well-known security triangle, which has ITS own evaluation criteria, the chosen evaluation metrics for this model were selected and assessed. Specifically, metrics such as point-to-point delay, resource utilization (CPU, memory, bandwidth), and average response time were employed.

Simulation Results

To assess, demonstrate, and validate the efficacy of the proposed model against other models, we evaluated our model across several scenarios using metrics such as end-to-end delay, responsiveness, and resource utilization. Network monitoring tools, including OpManager, Ping Plotter, and Zabbix, were employed to extract more reliable outputs.

In the chart, Figure 5, data with varying payload sizes were transmitted to illustrate the impact of increasing data size on the network's end-to-end delay.

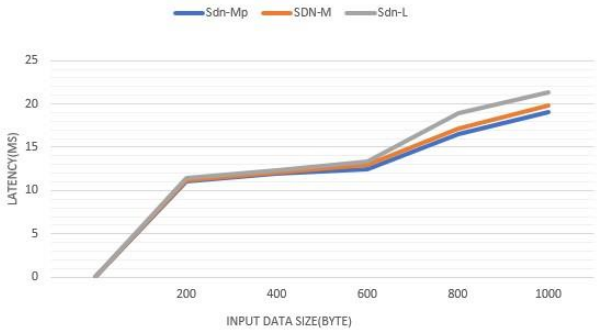


Fig. 5. Packet transmission latency of the proposed SDN VS. Non-SDN models. A comparission on different packet size.

As observed, all three models exhibit similar point-to-point delays. The underlying reason is that in SDN-based models, establishing an overlay tunnel introduces some overhead to transmitted packets; however, this overhead diminishes as the packet size increases, reducing the negative impact. Moreover, reductions in path computation time and continuous monitoring of existing paths, with the selection of the path with the lowest delay, in the SDN-generated models, lead to lower overall delay for larger packet sizes.

The effect of increasing the number of tasks or active network connections on point-to-point delay is clearly visible in Figure 6. The communications enabled by SDN networks, together with better path selection, utilize all available paths according to bandwidth and quality, effectively exploiting network communications capabilities. In other words, these models distribute network traffic load more efficiently. As the network topology becomes closer to a complete graph, traffic becomes more evenly distributed, leading to more optimal bandwidth utilization and, consequently, lower delays.

The simulation result in Figures 5 and 6 shows that the deployment of a full mesh network, ensure optimal inter-operability in IoV network and fault tolerant inter-communications. Thus, balanced bandwidth distribution, confirm network stability which play an important role in latency reduction, network availability, and security concerns in the proposed SDN-based IoV network. Moreover, creating communication tunnels and encrypting transmitted information will play an important role in enhancing confidentiality.

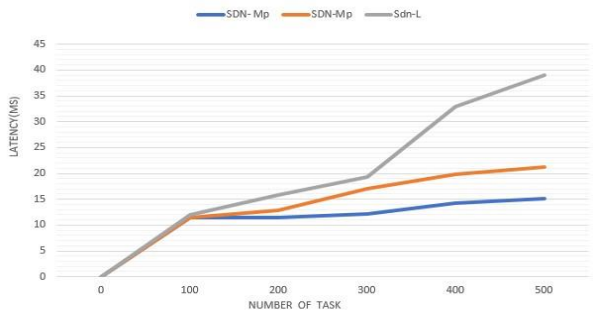


Fig. 6. Packet transmission latency VS. Number of packets. A comparison for the proposed model and Non-SDN models

Figure 7 shows the computational resource utilization across the implemented models. Overlay-based SDN networks reduce the consumption of local computational resources (memory and processor) by offloading computations to the central controller. Additionally, overall resource usage decreases due to the elimination of redundant or local routing computations, thereby reducing provisioning costs.

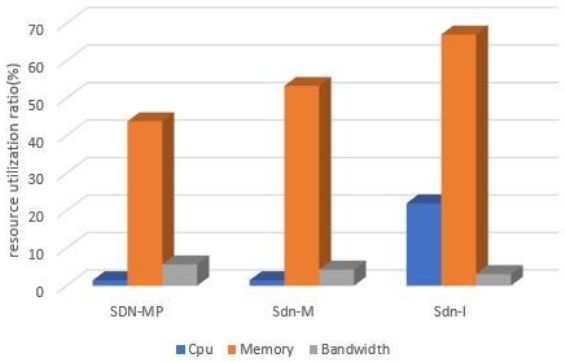


Figure 7: Graph of computing resource and bandwidth usage in the proposed model and non-SDN scenarios.

As shown in Figure 7, minimizing the resource consumption in the same scenarios depicts that the proposed model outperforms the other methods in resource shortages as well as starvation concerns. The proposed model ensures the optimal resource utilization, network availability, as well as security concerns. Figure 8 shows the response time evaluation for SDN-L, SDN-M, and SDN-MP. Results verify that the proposed model has a better response time, and service availability.

SDN-based models can select routes that minimize exposure to distance and detrimental factors (e.g., delays, packet loss, etc.) by choosing better paths.

Conversely, the SDN network can achieve shorter response times by preselecting optimized routes and reducing the time required to compute new paths. Traffic-aware policy implementation can further improve the response times in SDN-based models. For example, policies can be developed that, when the packet loss rate exceeds 2%, the receiver at the destination starts recovering information, which avoids sending out redundant information and consequently reduces fluctuations in network jitter.

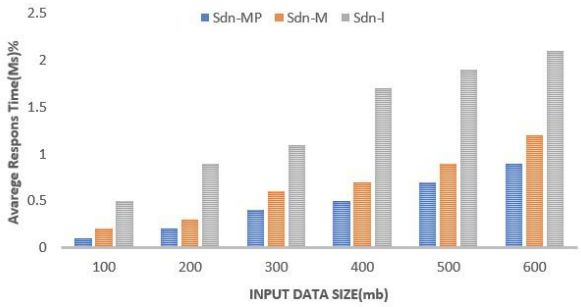


Fig. 8. Average network response time comparison in the proposed SDN and Non-SDN

Overall, through a comprehensive review of the charts and the evaluation of point-to-point delay and response time metrics, it can be concluded that the SDN overlay models offer superior security-related attributes, such as availability and confidentiality, compared to networks that do not

employ SDN overlays. This improvement stems from the structural advantages of SDN networks, which substantially enhance key network factors affecting security. Additionally, evaluations indicate that implementing functional, need-based policies for customizing IoV networks can render these networks more efficient, scalable, and secure.

V. Conclusions and Future Work

Attacks in IoV networks span a wide range and can frequently occur in vehicular networks. Issues such as the use of versatile malicious software, unauthorized data collection, manipulation of on-board units, transmission of malicious messages, traffic misdirection, or excessive consumption of computing resources, identity forgery, eavesdropping, and more can all pose serious threats to vehicular networks. Consequently, security strategies in these networks must be considered holistically and comprehensively. Developing methods that can identify legitimate users of these networks or keep the network away from unauthorized access can be highly important.

By securing the network infrastructure and establishing secure tunnels, security can be extended to different zones of the network. Similarly, by implementing security policies using the capabilities of SDN networking, SDN-enabled networks, it possible to impose restrictions on traffic, control the use of network resources, and manage the network infrastructure.

The proposed model is based on LTE communications and has been implemented under a city-scale simulation, such as Tehran, with the BTSs in Tehran configured in two forms: some BTSs utilize infrastructural connections such as fiber-optic links, while others lack such infrastructural connectivity. Among the discovered paths, those with fiber-optic infrastructure provide stronger links and lower delay.

The model could achieve improved performance by leveraging 5G communications and broader coverage. This direction can be pursued as a research topic for future work.

References

[1] X. Hou *et al.*, "Reliable computation offloading for edge-computing-enabled software-defined IoV," (in eng), *IEEE Internet of Things Journal,* vol. 7, no. 8, pp. 7097-7111, 2020. doi: 10.1109/JIOT.2020.2982292

[2] A. J. Kadhim, S. A. H. Seno, J. I. Naser, and J. Hajipour, "DMPFS: Delay-efficient multicasting based on parked vehicles, fog computing and SDN in vehicular networks," *Vehicular Communications,* vol. 36, p. 100488, 2022. doi: https://doi.org/10.1016/j.vehcom.2022.100488

[3] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE transactions on intelligent transportation systems,* vol. 22, no. 6, pp. 3832-3840, 2021, doi: 10.1109/TCSS.2023.3343084

[4] A. Hemmati and M. J. A. I. Zarei, "UFC3: UAV-aided fog computing based congestion control strategy for emergency message dissemination in 5G internet of vehicles," vol. 7, no. 3, pp. 456-472, 2024, https://doi.org/10.1007/s42154-024-00284-1

[5] A. Hemmati, M. Zarei, A. M. Rahmani, "Big data challenges and opportunities in Internet of Vehicles: a systematic review," vol. 20, no. 2, pp. 308-342, 2024. https://doi.org/10.1108/IJPCC-09-2023-0250

[6] P. K. Tiwari *et al.*, "A Secure and Robust Machine Learning Model for Intrusion Detection in Internet of Vehicles," *IEEE Access,* 2025, doi: 10.1109/ACCESS.2025.3532716

[7] M. M. A. Muslam, "Enhancing security in vehicle-to-vehicle communication: A comprehensive review of protocols and techniques," (in eng), *Vehicles,* vol. 6, no. 1, pp. 450-467, 2024, doi: 10.3390/vehicles6010020

[8] Y. Wang, A. Mahmood, M. F. Mohd Sabri, and H. Zen, "Towards distinguishing trust based attacks in an IoV network," *Journal of King Saud University Computer and Information Sciences,* vol. 37, no. 4, pp. 1-15, 2025, doi: https://doi.org/10.1007/s44443-025-00037-y

[9] K. N. Tripathi, A. M. Yadav, S. Nagar, and S. Sharma, "ReTrust: reliability and recommendation trust-based scheme for secure data sharing among internet of vehicles (IoV)," *Wireless Networks,* vol. 29, no. 6, pp. 2551-2575, 2023, doi: 10.1007/s11276-023-03336-2

[10] H. Cui and X. Yi, "Secure Internet of Things in cloud computing via puncturable attribute-based encryption with user revocation," *IEEE Internet of Things Journal,* vol. 11, no. 2, pp. 3662-3670, 2023, doi: 10.1109/JIOT.2023.3297997

[11] T. Cao, J. Yi, X. Wang, H. Xiao, and C. Xu, "Interaction trust-driven data distribution for vehicle social networks: A matching theory approach," *IEEE Transactions on Computational Social Systems,* vol. 11, no. 3, pp. 4071-4086, 2024, doi: 10.1109/TITS.2020.3048844

[12] D. Das, S. Banerjee, W. Mansoor, U. Biswas, P. Chatterjee, and U. Ghosh, "Design of a secure blockchain-based smart iov architecture," in *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*, 2020, pp. 1-4: IEEE, doi: 10.1109/ICSPIS51252.2020.9340142

[13] M. Shahzad, L. Liu, A. Kaushik, I. Bibi, and N. E. Belkout, "Fair switch selection for large scale software defined networks in next generation internet of things," (in eng), *Telecommunication Systems,* vol. 88, no. 2, pp. 1-14, 2025, doi: https://doi.org/10.1007/s11235-025-01290-2

[14] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security challenges in internet of vehicles (IoV) for ITS: A survey," (in eng), *Tsinghua Science and Technology,* vol. 30, no. 4, pp. 1700-1723, 2025, doi: 10.26599/TST.2024.9010083

[15] S. R. Pokhrel, "Software defined internet of vehicles for automation and orchestration," (in eng), *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 6, pp. 3890-3899, 2021, doi: 10.1109/TITS.2021.3077363

[16] A. Akbar, M. Ibrar, M. A. Jan, L. Wang, N. Shah, and H. H. Song, "SeAC: SDN-enabled adaptive clustering technique for social-aware internet of vehicles," (in eng), *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 5, pp. 4827-4835, 2023, doi: 10.1109/TITS.2023.3237321

[17] M. T. Abbas, A. Muhammad, and W.-C. Song, "SD-IoV: SDN enabled routing for internet of vehicles in road-aware approach," *Journal of Ambient*

Intelligence and Humanized Computing, vol. 11, no. 3, pp. 1265-1280, 2020, doi: https://doi.org/10.1007/s12652-019-01319-w

[18] L.-A. Phan, D.-T. Nguyen, M. Lee, D.-H. Park, and T. Kim, "Dynamic fog-to-fog offloading in SDN-based fog computing systems," (in eng), *Future Generation Computer Systems,* vol. 117, pp. 486-497, 2021, doi: https://doi.org/10.1016/j.future.2020.12.021

[19] A. J. Kadhim and S. A. H. Seno, "Maximizing the utilization of fog computing in internet of vehicle using SDN," (in eng), *IEEE Communications Letters,* vol. 23, no. 1, pp. 140-143, 2018, doi: 10.1109/LCOMM.2018.2878710

[20] B. Alaya and L. Sellami, "Toward the design of an efficient and secure system based on the software-defined network paradigm for vehicular networks," (in eng), *IEEE Access,* vol. 11, pp. 43333-43348, 2023, doi: 10.1109/ACCESS.2023.3264808

[21] A. A. Khadir and S. A. H. Seno, "SDN-based offloading policy to reduce the delay in fog-vehicular networks," (in eng), *Peer-to-Peer Networking and Applications,* vol. 14, no. 3, pp. 1261-1275, 2021, doi: https://doi.org/10.1007/s12083-021-01111-8

[22] R. Kait, S. Kaur, P. Sharma, C. Ankita, T. Kumar, and X. Cheng, "Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities," *Expert Systems,* vol. 42, no. 1, p. e13561, 2025, doi: https://doi.org/10.1111/exsy.13561

[23] H. M. Islam *et al.*, "Revisiting ONE Simulator in IoV Research: Seeing the Forest Through the Trees," *IEEE Access,* 2025, doi: 10.1109/ACCESS.2025.3552026

[24] S. R. Pappu and K. C. Chilukuri, "SDN controller selection and secure resource allocation," (in eng), *IEEE Access,* 2025, doi: 10.1109/ACCESS.2025.3565117