IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 March 2023, accepted 29 March 2023, date of publication 5 April 2023, date of current version 8 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3264808

RESEARCH ARTICLE

Toward the Design of an Efficient and Secure System Based on the Software-Defined Network Paradigm for Vehicular Networks

BECHIR ALAYA[1,2] **AND LAMAA SELLAMI**[1,3]

[1]Department of Management Information Systems and Production Management, College of Business and Economics, Qassim University, Buraidah 51452, Saudi Arabia
[2]Hatem Bettaher Laboratory, IRESCOMATH, University of Gabes, Gabes 6029, Tunisia
[3]CONPRI Laboratory, University of Gabes, Gabes 6029, Tunisia

Corresponding author: Bechir Alaya (b.alaya@qu.edu.sa)

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia for funding this research work through the project number (QU-IF-4-4-1-25472). The authors also thank to Qassim University for technical support.

ABSTRACT The advent of Intelligent Transport Systems (ITS) has led to the appearance of vehicles increasingly connected to their environment on global road networks. Due to the strict requirements for low latency and secure interactions in a vehicular environment, the proposal of new architectures is a crucial topic for discussion. This paper aims to develop a vehicular network using several access technologies based on SDN (Software Defined Network) paradigm, to take advantage of the capacities of the various access networks and provide flexibility in their control and management. Confidentiality, integrity, and authentication are essential services to prevent an adversary from compromising the security of vehicular networks. Therefore, good security and privacy management system is necessary to ensure this protection. We represent then a hybrid SDN-VANET architecture that can address all of the challenges we mentioned earlier. We are in the process of implementing a dynamic approach to optimize the positioning of controllers according to changes in network topology due to fluctuations in road traffic. We will also detail the topology estimation service based on machine learning techniques to provide network control functions with potential insight into the future state of the network, unlocking proactive and intelligent network control. We also provide a scheme that prevents and informs about basic and compound attacks and reacts to the privacy and security conditions of the vehicular network, managing the requirements of security management systems. The simulation results showed the effectiveness of the proposed schemes in terms of message loss rates, packet delivery rates (PDR), Round Trip Time (RTT), and delays. With used our scheme, the performance of the network is improved when SDN triggers the change of the RSU entity. Such as we notice that the average RTT is lowered by 68 ms and that the PDR remains around 94%. We also notice with the integration of the security and privacy scheme (SPS) that the performance of the network is improved, the average RTT is reduced by 51 ms and the PDR persists around 99%.

INDEX TERMS Vehicular networks, intelligent transport system (ITS), software defined network (SDN), privacy, security.

I. INTRODUCTION

The convergence of microelectronics and wireless communication technologies has allowed the creation of a combination of embedded systems and distributed systems that have generated Wireless Sensor Networks (WSN). WSNs are increasingly used in large system applications in a variety of fields: military, environment, health, and habitat grown tremendously to be one of the most essential components of the Internet of Things (IoT) [1]. Vehicle-to-vehicle communication (V2V communication) is the wireless transmission of data between vehicles (see Figure. 1). It is one of the main

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

applications of communicating objects via a specific network called VANET (Vehicular Ad hoc Network). The concept of vehicular networks opens up different types of communications to meet the needs of the Intelligent Transport System (ITS). In another parallel axis, network topologies have evolved and have given rise to the SDN (Software Defined Network) architecture which is famous for the separation between the data plane and the control plane. We can present SDN as the first network architecture that offers an intelligent materialization transformation to the software world and the hallmark of virtualization. SDN is the new networking paradigm with great potential to increase the efficiency of network management. SDN offers great flexibility and facilitates innovation in networks thanks to programmability. The key concept of SDN is the separation of the data plane and the control plane. Unlike traditional IP networks, routers perform both packet forwarding and routing computation, the routing function is moved from the routers to the SDN controller. In the SDN architecture, the switches only perform the data transfer function based on the rules established and installed by one or more SDN controllers. There has been a lot of research that has tried to apply SDN to VANET, with the objectives of quality of service, QoS (Quality of Service), mobility, security, etc. Secure communication on the road is the key to reviewing and validating the use of SDN in the road network [4]. It is therefore within this framework that this work falls, the contributions of which aim to develop the concept of VANET defined by SDNET Software (Software Defined Network to VANET). Our goal is to secure the SDN network in a VANET environment, it is above all necessary to understand the technology and design a light solution (in terms of the execution time of cryptographic operations). Defining defense techniques and acquiring the required skills are therefore at the heart of the security challenges of vehicular networks.

We represent the first step in creating a hybrid SDN-VANET architecture that can address all of the challenges we mentioned earlier. We are in the process of implementing a dynamic approach to optimize the positioning of controllers according to changes in network topology due to fluctuations in road traffic. We will also detail the topology estimation service based on machine learning techniques to provide network control functions with potential insight into the future state of the network, unlocking proactive and intelligent network control. Vehicle communications will allow drivers to be warned early enough of possible dangers thanks to sensors installed in vehicles, or located at the edges of roads and control centers [5], [6]. Vehicular networks have been designed to bring many advantages, such as the reduction of accidents, the comfort of drivers and passengers, the ease of payment for certain services such as parking, gasoline, games, and the online network, audio, and video downloads, etc. These applications make it possible to exchange data that can affect the behavior of conductors and thus modify the topology of the network. Thus, this means that there is a risk of attack by malicious users who can alter the messages exchanged on the network [7]. These VANET networks are still vulnerable to attacks such as Sniffing, Wardriving, Warchalking, Denial of Service, Traffic Blocking, Masquerade, Impersonation, Illusion, etc. [8]. The exchanges between the different types of objects in a VANET can give rise to internal or external security attacks [9], [10]. It is therefore essential but difficult to design an effective system that preserves the security and confidentiality of information exchanged between vehicles on VANET networks. To address security and performance issues, we are introducing a secure and intelligent detection scheme with strong privacy preservation, allowing a VANET user to securely receive and share messages. In summary, the paper's contributions are overviewed by the following points:

1) Creating of hybrid SDN-VANET architecture
2) Proposal of a dynamic approach to optimize the positioning of controllers according to several constraints
3) Description of topology estimation service based on machine learning techniques.
4) Introducing a new secure and intelligent detection scheme to securely receive and share messages.

The simulation results demonstrate that with a configuration of our suggested schemes, we have better results in terms of message loss rate, packet delivery rate, and delay reduction.

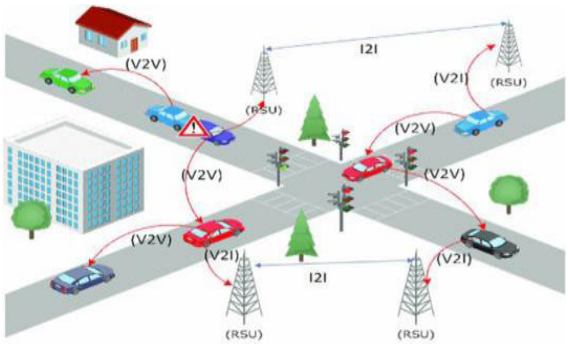

FIGURE 1. The architecture of VANET.

The rest of the paper is organized as follows: Section II highlights the patterns of Software Defined Networks (SDN). In section III, we introduce our first scheme. Section IV describes our privacy and security scheme. Section V evaluates the solutions. Finally, Section VI concludes the paper and recommends.

II. LITERATURE REVIEW

We mainly focus on work involving the adoption of SDN as an architecture for vehicular networks. This paradigm mainly aims to separate the data plane from the control plane. The success and achievements it has shown in these networks have attracted the attention of the community and several works are interested in its adoption in other types of networks, this is particularly the case of vehicular networks. Various scientific research, industrial and standardization organizations are interested in improving them by proposing new architectures and new mechanisms to efficiently support ITS services.

A. SDN INTEGRATION IN VEHICULAR NETWORKS

The SDN adoption paradigm for VANET networks is primarily aimed at separating the control plane from the data plane in the VANET environment. This paradigm has revolutionized wired network architectures and it has been widely adopted in the majority of infrastructures (e.g. data center networks, campuses, etc.). The success and achievements he has shown in these networks have caught the attention of the community and several works are interested in its adoption in other types of networks. This is particularly the case with VANET networks. These networks form the main foundation of an intelligent transport system

With this in mind, the authors of [11] proposed an ad hoc communication control between vehicles (V2V) and communications between vehicles and RSU (V2I) based on SDN. The SDN controller represents a single point of failure (SPOF). To address this problem, the authors proposed a replication strategy based on a local controller onboard the vehicle for efficient routing in the event of loss of connectivity with the controller. In our work, we propose an architecture that improves the support of ITS services by taking advantage of the advantages of the SDN paradigm. Our approach evokes the advantage of being able to dynamically reserve resources for a demanding security-type service. Other routing algorithms have also been proposed in [12], [13], and [14]. Such as SDN centrally calculates the optimal routing paths. The performance of the proposed approaches has surpassed the other approaches. The authors of [15] proposed SDN-based network architecture for geo-diffusion in VANET networks. In this architecture, the RSU entities are Open Flow compatible (communication standard between controllers and programmable nodes).

Truong et al. [16] explored the use of Fog Computing in an SDN-VANET architecture. Their proposal called FSDN integrates Fog computing to support constraining services in terms of latency as well as those based on location.

The authors of [17] proposed an approach based on distributed controllers. Their goals were to solve collision problems in very dense environments. Therefore, the distribution of the control plane ensures efficient data delivery by improving the scalability of the network. On the other hand, the proposed approach implements a data plan composed of single network technology, namely an RSU network in DSRC/WAVE technology using a cellular network as a control network. In [18] the authors proposed to implement software-defined network (SDN) technology in VANET networks. Their goal was to avoid the complexities and limitations of basic VANET structures. The authors highlighted SDN-VANET, services and challenges, attacks and applications, benefits, and finally how it works. Similar to the proposal of [16], the authors of [19], and [20] have proposed some approaches that support the most efficient VANET services, based on an SDN controller. In the work of [21] and for effective network control and supervision of vehicle dynamics, the authors have listed all the opportunities suggested by the use of data and the implementation of machine learning. The authors of [22], and [23] focused their work on controlling the VANET network via SDN. They based their work on learning mechanisms. On the other hand, the data considered comes mainly from the measures reported by the data plane nodes and is not enriched with external data.

In the next subsection, we will present some related works devoted to finding the best strategy for placing controllers in vehicular networks.

B. SDN LOCATION STRATEGY

We review the related work dedicated to finding the best placement strategy (the placement of controllers in the network and the assignment of vehicle nodes to each chosen controller) that optimizes one or more performance metrics.

Most of the literature work has considered routing nodes and latency between SDN controllers as a primary metric. Other metrics were considered, such as load balancing, controller capacity, communication latency between controllers, power consumption, and cost of deployment [24], [25], [26], [27].

Heller et al. [28] initially investigated the effect of SDN controller location on network performance. The authors agreed that better localization of the SDN controller significantly reduces average latency. Researchers have studied the optimization of latency between nodes and SDN controllers [29], based on a modification of the K-means method. Also, the authors of [30] proposed an approach based on a linear formulation to analyze the trade-off between load balancing and latency.

Likewise, the authors of [31] have proposed to employ the Bargaining Game to find a compromise between three factors, namely, the latency between the switches and the controllers, the latency between the controllers, and load balancing between controllers. Multi-objective optimization also has been taken into account by [32]. Based on the Pareto optimum, the authors have introduced an optimal localization of controllers SDN. They focus on the resilience of controllers. To avoid computational overloads, an extension of this work based on a heuristic approach is proposed in [33].

However, the location of the controllers is static in the works cited above relates to a static placement, that is to say, the location of the controller is calculated only once before being fixed on the network. Note that with an unforeseeable change in the network load, the performance of the controllers will no longer guarantee the expected performance. To remedy this type of problem, studies have proposed to enhance the dynamics of network traffic to periodically adapt the location of the controllers.

To balance the load on SDN controllers, the authors of [34] proposed a switch migration approach. The results showed that the proposed approach reduced the load disparity between SDN controllers.

Recently, the SDN paradigm has been extended to other types of networks, such as IoT networks [35], [36], [37], WSN networks, cellular networks, etc. The problem of the placement of controllers has been the subject of studies in

these fields, namely wireless networks [38], the LTE cellular network [39], and vehicular networks [40]. The problem is different from that of wired networks, especially when the southern interface (i.e. South-Bound Interface (SBI)) considered is as of the wireless type. The quality of the wireless links is a key element in determining the subset of links to use to connect the controller to the nodes. In addition, the location of users is also crucial in determining the request rate per eNodeB entity in cellular networks, a metric necessary for provisioning SDN controllers. In this study, we focus on vehicle networks programmable via SDN (SDVN). In this context, the fittest study of the controller placement problem was recently proposed by Liyanage et al. [38]. They focus on minimizing latency between nodes and controllers. Their approach consists in favoring the RSUs located at strategic places (ie road intersections with regularly heavy road traffic) to accommodate the controllers. This choice is motivated by the fact that vehicles travel less quickly in overcrowded intersections. This increases the likelihood that vehicles will stay closer (direct coverage) to their controller for a long time.

Most of the work in the literature dealing with the problem of controller placement focuses on networks other than vehicular networks. Different optimization methods are used to solve the problem. And different metrics are studied, mainly the latency between the controller and the routing nodes, and the capacity of the controllers. To continue to guarantee the best performance, regardless of the evolution of network traffic, the adaptive/dynamic approach has been introduced in the wired context. However, very little analysis is provided regarding the impact of controller changes on overall network performance. The problem has recently been studied in other emerging areas, particularly in the context of vehicle networks programmable via SDN. The first work of the mature dealing with this problem in the vehicular context was in [40]. It offers a static placement of controllers in RSU entities having a strategic location. However, with traffic fluctuations, the fixed location of controllers becomes ineffective for the overall performance of the VANET network. To overcome this problem, we propose a dynamic approach to place the controllers in an SDVN context. Our idea will be to adapt the location of SDN controllers according to the dynamics of network traffic.

Subsequently, we review some related works dedicated to the search for the best protection schemes against attacks in vehicular networks.

C. SECURITY ISSUES OF VANETS

Several protection mechanisms focus on attacks directed at VANET network communications and their vulnerabilities, particularly in information routing and its integrity [20], [41], [42]. A distributed approach is presented by Zaidi et al. [43] to detect Sybil attacks and the dissemination of false information from malicious vehicles. Each vehicle uses the Greenshields model [44] which describes the relationships between speed, density, and the flow of vehicles per hour on a road. The relationship between the speed and density of vehicles in an uninterrupted flow is described there as a linear relationship in which density is negatively correlated with speed. In other words, the more vehicles there are on a road, the lower their speed. Zeng et al. [45], [46] seek to detect denial-of-service, black hole, and wormhole attacks, but also Sybil attacks operating on VANETs networks as well as traffic generated by malware from the ISCX2012 data corpus [47]. They present an approach based on deep neural networks and compare the detection capacities of three neural networks LSTM [48], CNN, and DeepVCM. The latter is itself made up of LSTM and CNN. They also compare the results of SVM algorithms and decision trees. They find that their method (DeepVCM) obtains better detection results than the other solutions studied while being more economical in storage.

The work presented by Aloqaily et al. [49] presents the use of a decision tree-based algorithm for intrusion detection. They offer a framework in which vehicles access the services offered by cloud services by communicating with an intermediate vehicle (cluster head) elected from a group (cluster) of nearby vehicles. Another example not directly related to the field of the vehicle is presented by Al Mamun and Valimaki [50]. This work focuses on the detection of anomalies in cellular networks at the level of the operator network and its management. They use a support vector machine to detect anomalies and apply a recurrent neural network (LSTM) to the detected anomalies to understand how the anomaly changes over time. They study anomalies based on key attributes of 4G networks such as the number of connection establishments between mobiles and the 4G core network or the handover ratio (or handover 6) that has taken place. V. Singh and K. Mahajan [51], [52], working on a review article on security issues in VANETs. The authors worked on the growing interest in VANETs but highlighted many security issues. Through the use of winning algorithms, Elliptic Curve [53], [54] offers scientific suggestions to improve public key cryptography and implements cryptographic systems for security.

Yuh-Min Tseng [55], worked on different Digital Signature schemes by not using any hash or message redundancy. The reason for this study was to save from Forgery Attacks that were proposed by Chang and Chang while working on digital signatures. The work was then of interest to all the security designers who worked mainly on hash functions that were conventionally available to save from outside attacks. The schemes of security were insecure largely. Alaya et al. [56] have proposed a distributed key management system for VANETs based on a symmetric cryptography scheme and clustering method. A promising approach for privacy protection in vehicular networks (VANET). This network model consists of 3 entities: (i) The Authorities (CA) which are responsible for the management of VANETs, generation, and revocation of keys. (ii) RSUs are responsible for distributing a group of private keys on a localized basis. (iii) The nodes are ordinary vehicles, each vehicle is equipped with

a GPS receiver and an OBU onboard unit responsible for all communication and calculation tasks. To guarantee the security of urban P2P VANET networks, the authors of [57] have proposed an efficient certification framework, where the trusted authority starts to initialize the system. Then, for node ., the mobile proxy sends it its private key and certificate. To detect routing attacks, the authors proposed an efficient cooperative neighbor × neighbor (CNN) detection system. This system can intelligently detect based on two phases {response requested and response to the request}. Asfara et al. [58] proposed a solution to secure communication between vehicles in a VANET environment with the presence of an SDN Controller and its advantages. The nodes in this topology reacted with the controller as a trusted Public Key Generator (PKG) entity and the RSUs as there are switches. The proposed security mechanism consists of 1) a registration procedure and 2) an authentication procedure / Session key generation. Al-Shareeda et al. [59] formalized a model of the system with social characteristics, i.e., human mobility, human group, and preferences in an ad hoc network that consists of a trusted authority (TA), stationary units (SU) deployed to the social space, and a large number of mobiles equipped with wireless technology in motion on social space. They proposed an efficient certificate scheme, where the TA issues the private key and the certificate. Based on proxy re-signature cryptographic technology [60], the node requests the re-signature key and then re-signs the certificates issued by the TA. A Blockchain-based authentication and revocation solution is proposed in [61], [62] to allow RSUs to verify the identity of a vehicle. For each vehicle, a pseudo-ID is obtained from the certification authority and then stored with the certificate in an immutable authentication Blockchain The authors of [63] introduced architectures and protocols for authentication in vehicular networks as well as the corresponding performance analysis. The solution proposed therein for authentication has been designed to meet not only the characteristics of service, mobility, connectivity, and topology of vehicular networks but also the operating characteristics of a vehicular network and the security requirements of all network services. An approach for optimizing the initial solution authentication transport has also been proposed.

The following subsection provides a summary of the different aspects taken into account in the articles cited above and shows our position concerning these related works.

D. RELATED WORK LIMITATIONS AND POSITIONING OF OUR APPROACH

The majority of works in the literature dealing with the problem of controller placement focus on wired networks. Different optimization methods were used to solve the problem. And different metrics are studied, mainly the latency between the controller and the routing nodes, and the capacity of the controllers. To continue to guarantee the best performance, regardless of the evolution of network traffic, the adaptive/dynamic approach has been introduced in the wired context. However, very few analyzes are provided regarding the impact of controller changes on overall network performance. The problem has recently been studied in other emerging fields, particularly in the context of vehicular networks programmable via SDN. We have presented the first work in the literature dealing with this problem in the vehicular context [40]. It proposes a static placement of controllers in RSU entities having a strategic location.

However, with fluctuations in road traffic, this static placement may no longer be effective. For example, a traffic jam in a given area can result in a high number of vehicles located far from deployed controllers. A detailed analysis of the limits of static placement in a vehicular context is presented next. To overcome this problem, we propose a dynamic controller placement in an SDVN context. The main idea is to adapt the placement of controllers according to the evolution of road traffic. Our analyzes are based on a realistic traffic scenario, compared to the small simplified network considered in [40].

Table 1 shows our positioning concerning the work presented above. Knowing that in table 1 the goals G1, G2, G3, and G4 respectively represent: Latency, Capacity, Reliability, and Replacement cost.

To show the limits of a static placement in an SDVN context, we use a realistic mobility trace to analyze the impact of road traffic fluctuations on the performance of the placement.

Figure. 2 illustrates a simplified road network, represented as a graph. Each node represents an RSU entity. The links represent the roads; each link is colored according to the

TABLE 1. Our positioning concerning the work presented above.

Ref	Nodes			Control Plane	Data-Guided Control
	Vehicles	RSU	BS		
[11]	√	√		Centralized	
[12]	√			Hierarchical	
[13]	√			Centralized	
[15]	√	√		Centralized	
[16]	√	√	√	Hierarchical	
[17]	√	√		Hierarchical	
[18]	√	√	√	Hierarchical	
[19]	√	√	√	Hierarchical	
[20]	√	√		Centralized	√
[21]	√	√		Centralized	√
Our Work	√	√	√	Hierarchical	√

Ref	Context	Goal				Approach	
		G_1	G_2	G_3	G_4	Static	Dynamic
[28]	WAN	√				√	
[29]	WAN	√				√	
[30]	WAN	√	√			√	
[31]	WAN		√			√	
[32]	WAN	√	√	√		√	
[33]	WAN	√	√				√
[34]	WAN	√	√				√
[35]	WAN	√	√		√		√
[36]	WAN	√		√			√
[37]	WAN	√	√				√
[38]	LTE-Net	√	√				√
[39]	VANET	√	√			√	√
[40]	VANET	√	√			√	
Our Work	VANET	√	√		√		√

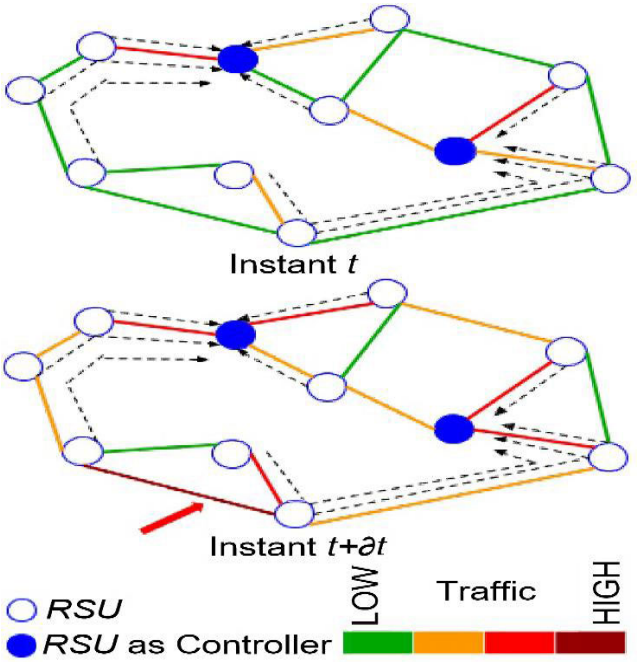

FIGURE 2. Simplified representation of road traffic fluctuations.

traffic density on each road. Blue nodes represent deployed controllers, and dotted lines represent node assignments to each controller. The evolution of traffic during the day implies variations in the number of vehicles and the distribution of vehicle density. For example, the roads and places used during working days differ from those on weekends. These variations mainly affect two measures, namely: *i*) the load on the controller (in the number of controlled nodes (vehicles)), and *ii)* the number of nodes far from their controller (in the number of hops), as shown in the graph colored from the right. Instanced controllers become overloaded (increased number of managed vehicles) and several nodes are located three hops away from their controllers (e.g. area pointed by red arrow). This results in increased latency between controllers and vehicles, as explained earlier.

III. SDN PARADIGM AND GENERAL DESCRIPTION OF THE PROPOSED ARCHITECTURE

This section presents the proposed architecture. We first present the SDN paradigm by describing the key principles and design choices that guided the development of this architecture. Finally, we analyze the various opportunities of the proposed architecture.

A. SDN PARADIGM IN A VANET ENVIRONMENT

In a VANET network, each network device is made up of a data plane and a control plane. The primary purpose of the data plane is the routing of data, while the control plane is responsible for all network control decisions, such as deciding from which interface data is routed. With conventional networks, the same device comprises the control plane and the data plane. Each plane makes its own decisions independently. However, the SDN paradigm recommends

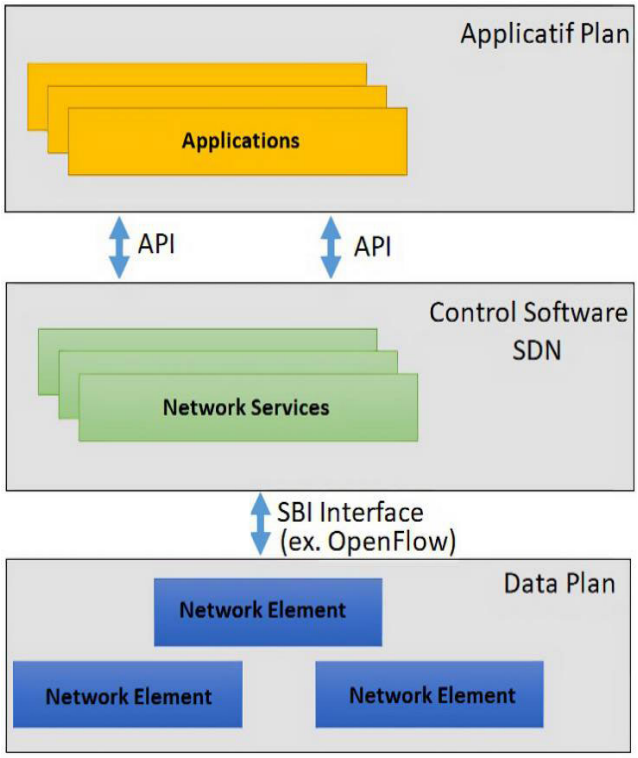

FIGURE 3. The global architecture of the SDN paradigm.

the separation of the control plane and the data plane. This is because network control functions are outsourced from network equipment and arranged in software components on dedicated external equipment called SDN controllers. Figure. 3 shows our global architecture of the SDN paradigm composed of an Application Plan, a Control Software SDN, and a Data Plan, such that the SDN Controller is the central element of our architecture. It communicates with the various nodes of the VANET network via a South-Bound Interface (SBI) protocol. While the Northbound Interface (NBI) protocol expresses the need for the SDN controller.

The SDN controller provides an abstraction of the underlying network to network applications and services and is responsible for setting the various network policies. The data plane is made up of routing nodes often referred to as PFE for Packet Forwarding Element.

B. GENERAL DESCRIPTION OF THE PROPOSED ARCHITECTURE

As the main basis, we integrate the SDN paradigm in our hybrid vehicle network service protection architecture. To improve the control of the VANET network and facilitate its management in addition to the advantages of hybridization, we still use the advantages of the SDN paradigm. Therefore, we can develop efficient VANET network protection algorithms

which will be based on knowledge of the environment of the vehicle nodes, the global state of the communication networks (Multi-RAT), and finally the capacity for dynamic control of the networks. These different data can come from

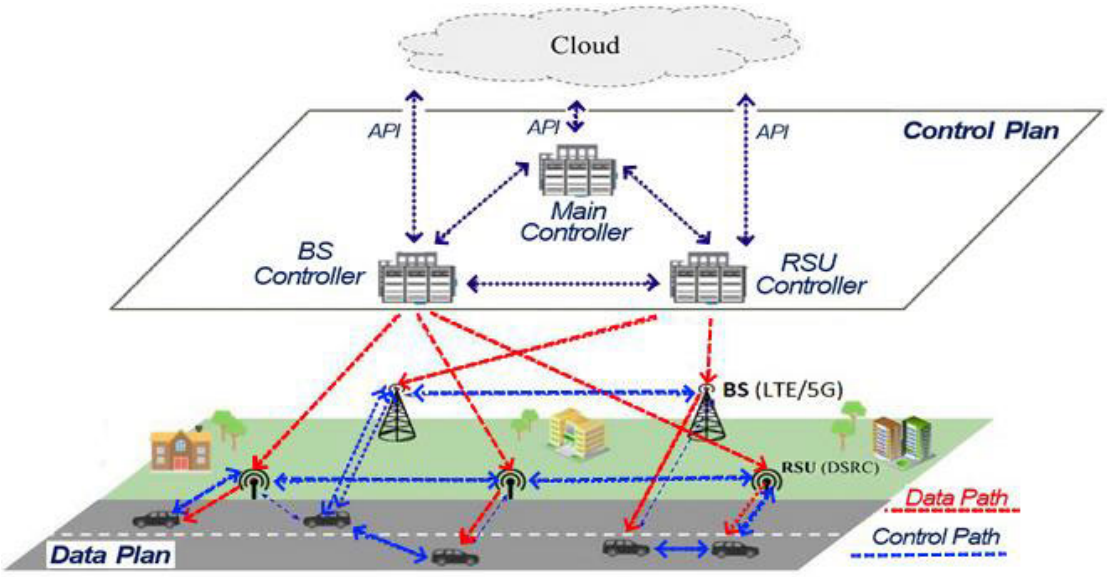

FIGURE 4. Global vision of the proposed architecture.

road authorities, VANET operators, etc. Our architectural goal is to separate the control plane from the data plane through intelligent integration of the SDN paradigm (see Figure. 4). Several policies are implemented by SDN controllers, maintaining the intelligence of the VANET network.

As shown in Figure. 4, the red and blue dotted lines distinguish the control paths and the data paths respectively. According to the instructions provided by the SDN controllers, the nodes of the data plane ensure the routing of the data. We can design three conceptual principles of our architecture, which are detailed in the following subsections.

1) HETEROGENEOUS DATA PLANE (MULTI-RAT) IN THE PROPOSED ARCHITECTURE

We can notice in Figure. 4, that the data plane consists of components programmable via SDN, such as RSUs, vehicle nodes, and finally base stations. This choice is motivated by the vision of hybridizing DSRC and cellular technologies to take advantage of their advantages and to couple their capacities to effectively support ITS services. We consider that vehicles are equipped with two or more network interfaces. For example, one interface to access the RSU network (DSRC) and another to access the cellular network (LTE / 5G). However, vehicle nodes are considered programmable via SDN, by default. The latest studies have shown the motivation of the SDN paradigm and that centrally computed routing is more efficient than distributed computed routing. According to the observed results of SDN controllers applied on VANET networks, it is clear that the vision offered by SDN can lead to an interesting reduction in the risk of collisions by controlling the transmission parameters. We assume that the interface posed in our architecture also allows performing the choice of wireless channels, power control, and routing. The difference between data plane nodes lies in the features supported by each node and their specific characteristics. From the perspective of the SDN controller, the nodes are transparently controlled according to a unified model.

2) HIERARCHICAL CONTROL PLAN

SDN controllers define the rules for different nodes in the data plane. It represents the essential element of our architecture which hosts the various control functions of the VANET network. Given the type of nodes and their locations, SDNs are connected to nodes.

We have three types of main controllers such as an RSU network manager, a cellular network manager, and a coordinator of various controllers. The choice of separating controllers by technology is motivated by the fact that each network could belong to a different actor. For example, the cellular network is managed by a mobile network operator and the RSU network is managed by city authorities or road network managers. Based on the joint control of VANET networks, we decided on a hierarchical manner for the control plane organization in our architecture. Indeed, from the data of each network, a global view of the communication infrastructure is constructed by the main controller. Note that the BS and RSU controllers define the specific rules to be implemented by each node of the network. While the main controller transmits to each controller the general behavior of the network. However, some network control decisions can be made by local controllers and may not require direction from the global controller. For example, horizontal handover operations (change of attachment point within the same network, e.g. $BS \leftrightarrow BS$). On the other hand, vertical handover operations (change of attachment point between two different $RSU \leftrightarrow BS$ networks) may require directives from the global controller. In any case, we assume that the various players agree to expose the information from their networks, necessary to perform hybrid control.

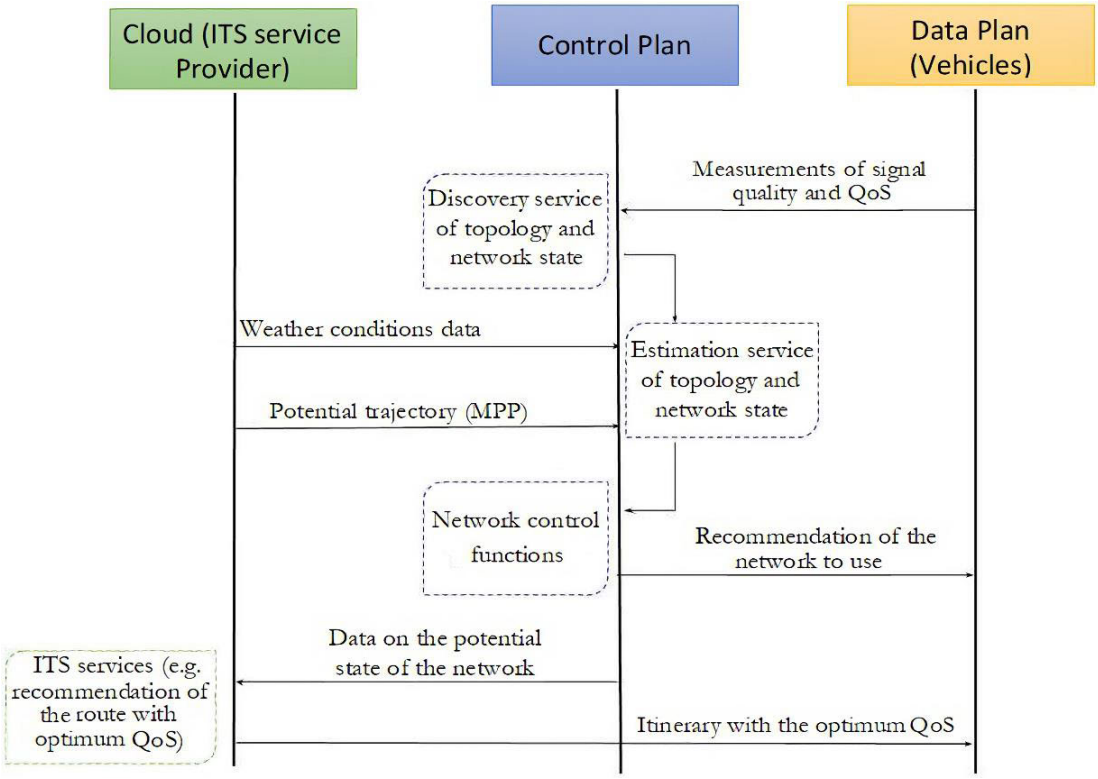

FIGURE 5. Data-driven control.

3) DATA-DRIVEN CONTROL

For more efficient network VANET control, SDN controllers can use data from external actors (such as route managers, VANET operators, etc.). This data is used to derive a potential view of the network status and to enrich the network overview.

We notice in Figure. 5 the data exchange between system actors, the control plane, and the data plane which represent the vehicle nodes for a detailed design of VANET services. To enrich the global vision built by SDN controllers, data plane data can be combined with external data. This service can leverage information about the potential trajectory of MPP (Most Probable Path) vehicles to derive potential network attachment points for a given vehicle, which will help estimate potential network load. These data can be provided by ITS service providers, part of their services of which are based on the vehicle's potential trajectory. We cite the example of the eHorizon driving assistance service [64], which provides vehicles based on their MPP with condition road information. On the other hand, the potential network condition estimation service can take advantage of additional input weather data to accurately predict signal and network quality for nodes in a given area.

The network selection function can take advantage of this potential network vision to effectively guide vehicles in choosing which communications network to use. This decision will be based not only on the current condition of the two networks but also on their potential condition. However, ITS service providers can design services based on potential network quality data. For example, the route recommendation service can take advantage of this data to recommend routes for vehicles that provide a better network service quality [65]. This property requires collaboration between the various systems actors for the data exchange.

C. ARCHITECTURE OPPORTUNITIES

The proposed architecture offers many opportunities in network control terms. They are mainly inherited from the properties of the SDN paradigm coupled with the advantages of vehicular communication technologies hybridization.

Network programmability contributes significantly to improving network quality of service management. Indeed, fine-grained programming of the network makes it possible to dynamically allocate resources at the scale of a flow [66]. In addition, it offers the possibility of reconfiguring and adapting to variations in the quality of service. This flexibility fully responds to dynamic variations in this type of network. This dynamic of topology caused mainly by the mobility of vehicles requires an adaptation of the transmission parameters. The topology control function can take advantage of the overall view of the network to quickly reconfigure the topology to minimize transmission problems (interference, collision, etc.). Algorithms providing joint control involving both topology control and QoS management can be designed to ensure optimal performance.

The global view of the network state allows efficient use of available network resources, which many algorithms can take advantage of. For example, network resource allocation

algorithms can take advantage of this insight to optimize the resource allocation of the various available networks. These algorithms can also take advantage of the potential view of the network state to optimize these networks' use. Other approaches provide load balancing between various networks and even prioritize the DSRC network to alleviate cellular network overload and minimize communication costs while meeting network service requirements.

In addition to major advantages in terms of the development of network control functions. The software nature of these functions provides flexibility in choosing which network control functions to perform in a given area and at a given time. Indeed, we can consider activating/deactivating a network control function depending on the environmental conditions. For example, for the network control functions ensuring routing based on multiple-hop links, the work of the literature reports that each algorithm is effective in particular conditions (environment (urban, rural, etc.), vehicle mobility (speed, density, etc.)) [67], [68]. Based on the overall view of the network and the environment in which the vehicles operate, controllers can decide which mechanism to put in place and therefore can activate the most appropriate control functions for each situation.

Finally, the software nature of network control functions offers the possibility of flexibly adding new control functions to adopt network management strategies. This flexibility property offers the prospect of system continuous evolution.

IV. SECURITY AND CONFIDENTIALITY SCHEME

We present, in this section, a confidentiality and security scheme applied to the ITS environment. This scheme is based on five steps that are presented as follows.

A. KEY AND CERTIFICATE SENT BY SDN

We assume that there is a Trusted Authority (TA) to initialize the whole system. We adopt AODV (Ad hoc On-Demand Distance Vector Routing) [69], as the routing protocol selected by SDN. We have {MesDem, MesRes, MesNot} in the format of the message "RREQ route request" [57], the three control messages which are initialized by SDN. The system will be initialized by SDN b performing the following steps.

1) The security parameters begin to initialize with the SDN by executing $R.Init(1^{\delta})$. Knowing that R represents all of the RSUs which receive an optimum of the replica messages. $R.Init(1^{\delta})$ allows for generating a bilinear environment $(t, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, i, \mathcal{F})$ where (δ, k) are the security parameters, $\mathbb{G}_1, \mathbb{G}_2$ two groups of order t, g_1 is the generator of $\mathbb{G}_1$, and g_2 is the generator of $\mathbb{G}_2$. The SDN selects $sands' in Z_t^*$ and calculates $x = g_1^s \in \mathbb{G}_1 and y = g_2^{s'} \in \mathbb{G}_2$. SDN then chooses a secure symmetric encryption algorithm $Enc(.)$, and a random number $k \in Z_t^*$ selected as a master key. Next, it chooses two secure cryptographic hash functions Ω_1, Ω_2 [70], [71], such as $\Omega_1: \{0,1\}^* \rightarrow \mathbb{G}_1$, as $\Omega_2: \{0,1\}^* \times \mathbb{G}_2 \rightarrow \{0,1\}^k$.
   a) Depending on confidentiality requirements, SDN selects $\Delta\varepsilon$ and decides the certificate validity at $\Delta\varepsilon$.
   b) SDN keeps the master key k as secret, and shares the system parameters in VANET $(t, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, i, \mathcal{F}, \Omega_1, \Omega_2, Enc(.), \Delta\varepsilon)$.

Suppose that we have a new vehicle node wishing to communicate with other nodes, for an RSU R_i in the cluster Cl_j [72], the SDN sends the certificate $Cert_{v_i}$, and the private key PK_{v_i} as follows:

1) SDN calculates $LID_{v_i} = Enc(ID_{v_i})$ which represents the login identity of the vehicle node with the master key k.
2) Then SDN defines the secret key $PK_{v_i} = \Omega_1\left(LID_{v_i}\right)$, the public key $GK_{v_i} = sg_1$, and an arbitrary number $\in \mathbb{Z}_t^*$.
3) Using the signature generation algorithm [73], [74], SDN generates the signature χ_{v_i}.
4) Finally and safely SDN generates LID_{v_i}, PK_{v_i}, *and* $Cert_{v_i}$. SDN keeps track of the mapping between $Cert_{v_i}$ and the veritable ID_{v_i}.

Using the function $R.\text{Monit}(\chi_{v_i}, g_1, GK_{v_i})$, the vehicle node v_i can verify the certificate $Cert_{v_i}$. We can discover then that our scheme can necessarily guarantee optimum confidentiality of the identity of the user of VANET by using this key distribution method.

B. THE CERTIFICATE UPDATE IN THE PROPOSED SCHEME

A restoration policy has been implemented in our proposed scheme. Such, SDN can offer several certificates for each vehicle node. However, these certificates should not be used immediately after they arrive from SDN in the VANET network. Note again that only the certificates issued by RSU R_i belonging to the Cl_j study clusters are valid. As already presented in [60], we adopt in our scheme the technology of proxy re-signature cryptography. This technology is based on requesting the re-signing key from all nodes of Cl_j (N_j) and then deciding whether the certificates issued by the SDN and those issued by itself are the same or not. Suppose we have a real-time cT_k, then to obtain the re-signature keys corresponding to R_i, the vehicle node v_i can use the Scert signature certificates. We then present an algorithm that details the updated certificate.

C. VERIFICATION AND SIGNATURE

The vehicle node v_i uses the signature algorithm SigAlg, to sign the three messages {MyDem, MyRes, MyNot}. Also note SigAlg represents: $\text{R.Sign}\left(\text{K}, PK_{v_i}, \text{MesDem}\right)$ Concat $h_{v_i,\text{MesDem}}$ where $\text{K} = \Omega_2(TP \cdot Cert_{R_j,v_i})$ represents the temporary key and TP is the time stamp, $Cert_{v_i}$ is the certificate of v_i issued by the SDN, and PK_{v_i} is the private key of v_i.

The other vehicle nodes wait for the receipt of the MesDem from v_i, then they begin to check if $Cert_{R_j,v_i}$ is valid. Then the vehicle nodes check if $\text{R.Check}(\text{MesDem}, h_{v_i,\text{MesRes}}, K)$ is true to accept the message m_i.

Algorithm 1 Certificate Update Algorithm

1. Select of Cert_{v_i}, GK_{v_i}, g_1
2. if (Cert_{v_i} isvalid) Then
3. Calculate: C, D, S Such as:
   $\text{C} = s' \cdot \text{GK}_{v_i}$; $\text{D} = s' \cdot g_1$; $\text{S} = \text{Enc}_C(\text{T}_k \text{concat} \text{Cert}_{v_i,k})$
4. else (Reject)
5. if (S is valid during the gap time $\text{T}_{k+1} \ldots \text{T}_{k+N_j}$) Then
6. Calculatethere $-$ signaturekey$\text{RK}_{v_i,k}$)
7. else (Reject)
8. if ($\text{RK}_{v_i,k}$ is valid) Then
9. Accept $\text{RK}_{v_i,k}$
10. else (Reject)

We can define the detection time for $TimeDet_{v_i}$ attacks from v_i based on the following conditions: the time it takes to send the message MesDem, the real environment of VANET, and the transmission power and bandwidth of the VANET network, as follows:

$$TimeDet_{v_i} = \text{TN}_{MesDem} - \frac{OT}{LS} \tag{1}$$

That: LS is the light speed, TN_{MesDem} is the send time of the message *MesDem*, and *OT* represents the optimum transmission. To optimize the number of erroneous decisions $TimeDet_{v_i}$ must be carefully calculated. We can conclude that this is probably an attack if and only if $TimeDet_{v_i} < 0$ (see algorithm.)

D. THE REQUESTED RESPONSE

A Vehicle node or RSU node $\in Cl_j$ sends a request (executes Algorithm. 2) to the nodes belonging to their routing table to check and detect the attacks. These attacks can in particular copy, modify or cut messages to send false messages. To execute the notification phase, the vehicle, and RSU nodes wait for the response to its requests.

We can summarize this phase by the following steps:

1) Using the primary key $\text{K} = \Omega_2 \left(TP \cdot Cert_{R_j,v_i}\right)$, and the private key PK_{v_i}, node v_i can sign the message. Also, he must wait for the time τ to elapse to minimize the chances of collisions. Then, as already noted in our Algorithm. 2. line from 1 to 5, sends to its neighbors a jump in its routing table.
2) The node v_i retrieves the encrypted control message MesRes from γ, after having received MesRes from v_j. As shown by algorithm 2, from lines 6 to 13, if the signature is valid & $TimeDet_{v_i} < 0$, it considers that the link with the node v_j is proven. Otherwise, it returns unproven to begin the notification phase.
3) If v_i decides to begin the notification phase, it prepares MesNot and deletes the adversary node v_j in its routing table at one jump. Then v_j sends MesNot to all its neighbors of the same Cl_j to delete the adversary node in its routing table. Finally, as noted in Figure. 6, each neighboring node broadcasts MesNot to all the nodes in its routing table.

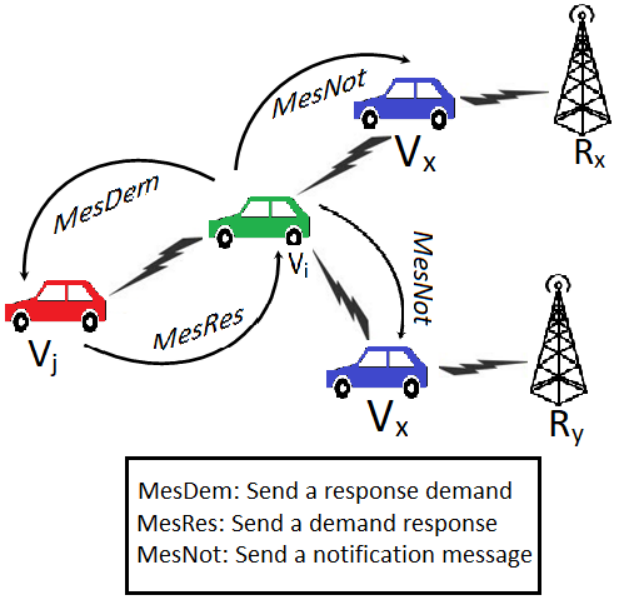

FIGURE 6. MesDem & MesRes.

In our scheme, by adapting the cryptographic technology of [60] a node cannot generate a correct signature for false certificates. Also, a node must limit the misuse of credentials, since a certificate $Cert_{v_i}$ is only valid during a fixed deadline.

Algorithm 2 The Requested Response Algorithm

1. Input: Current timestamp & *MesDem*
2. Calculate $\text{K} = \Omega_2 \left(TP \cdot Cert_{R_j}\right)$
3. Calculate:
   $\varphi = R.Sign\left(K, PK_{v_i}, MesDem\right) concath_{v_i,MesDem}$
4. Select the shortest time between two messages (τ)
5. Sharing of φ
6. Select and retrieve the MesRes message from Cl_j, when a node detects an encrypted MesRes control message
7. Calculate $\pi =$ R.Check(MesRes,$h_{v_i,\text{MesRes}}$, K)
8. if (π is valid) Then{
9. *Calculate*:$TimeDet_{v_i} = \text{TN}_{MesDem} - \frac{OT}{LS}$
10. If $TimeDet_{v_i} < 0$ Then
11. return (uncertain)
12. else return (proved)
13. else return (uncertain)}

E. RESPONSE TO THE ATTACK DETECTION DEMAND

A node v_j executes the Request-Response algorithm (Algorithm. 4). in the event, that it receives an attack detection request. Thus, a response to the detection request is summarized as follows: When the node v_j receives the encrypted control message *MesDem*, φ receives and decides whether it's signature R.Check(MesRes,$h_{v_i,\text{MesRes}}$, K) is valid or not. Then, if it is not valid, the node v_j sends a requested response to v_i, otherwise the node v_j signs the response

Algorithm 3 The Requested Response Algorithm

1. Input: The attack node & MesNot
2. Calculate γ= R.Sign $\left(\mathrm{K}, PK_{v_i}, \mathrm{MesDem}\right)$ Concat$h_{v_i,\mathrm{MesDem}}$
3. if $(v_x \in (1 - jumpofv_i))$ Then
4. In the routing table of v_i at $1 - jump$, remove v_x
5. return ()
6. else return ()
7. Output: γ available for transmitting

Algorithm 4 The Requested Response Algorithm

1. Input: M the message of encrypted control *MesDem*
2. Selected Current times tamp
3. Calculate: K $=\Omega_2\left(TP \cdot Cert_{R_j,v_i}\right)$
4. Calculate $\gamma =$ R.Sign $\left(\mathrm{K}, PK_{v_i}, MesDem\right)$ Concat$h_{v_i,\mathrm{MesDem}}$
5. if (v_i*receiveMesDem*)) Then
6. retrieve *MesDem* from M
7. Calculate π= R.Check(MesRes,$h_{v_i,\mathrm{MesRes}}$, K)
8. if (π = *true*) Then
9. send-response (γ, v_i)
10. Else Response_demanded ()
11. Output: γ the encrypted control message MesRes

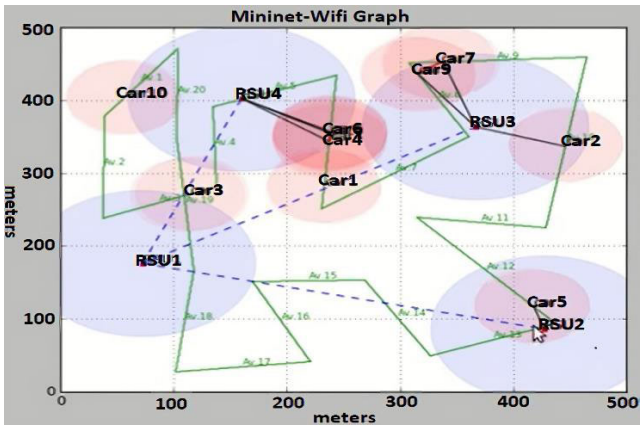

FIGURE 7. Simulation Scenario - Phase 1.

R.Sign $\left(\mathrm{K}, PK_{v_i}, \mathrm{MesDem}\right)$ Concat$h_{v_i,\mathrm{MesDem}}$ and returns it to v_i.

V. EXPERIMENTAL RESULTS

The experiment aims to show how the global view of the vehicular network established at the level of the controller, combined and enriched with the data provided by the external actors, allows more targeted and more effective control of the network to support ITS services efficiently.

We show through evaluations how the SDN controller can leverage its global view of current and potential network loads to guide the node in selecting the network attachment point with the best-expected performance.

We first present the simulation tools supporting the simulation prerequisites of our architecture. Furthermore, we describe the tools chosen for our studies. Finally, we present the obtained simulation results.

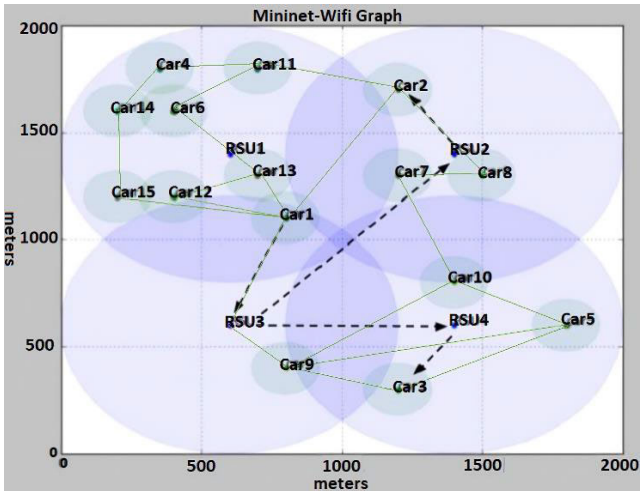

FIGURE 8. Simulation Scenario - Phase 2.

TABLE 2. Simulation parameters.

PARAMETERS	Setting
Simulation area (Phase 1)	500 m × 500 m
Simulation area (Phase 2)	2 km × 2 km
Paquet Size	1500 bytes
Traffic type	UDP
Vehicle speed	0-50 km/h
PHY/MAC Layer	IEEE 802.11p
Buffer size	41 Mbytes
Measuring interval	1 s
Bandwidth	10 Mbytes/s

A. SIMULATIONS DESCRIPTION

To study and evaluate the proposed architecture for vehicle networks programmable via SDN, the simulation environment must combine (in the majority of cases) both: (*i*) support for SDN programmable networks, (*ii*) a wireless communication medium, and (*iii*) a vehicular mobility medium.

To meet these simulation needs, we choose the use of MiniNet-WiFi [75]. We opt for a VANET network under SDN control, which consists of four RSU entities, each with a coverage of 600 m.

We have chosen a two-phase simulation. First, a phase where the number of vehicle nodes is average (medium load), then another phase where the number of vehicle nodes is high (overloaded network).

We consider 10 vehicles in the first phase, generating a VANET network in an area of 500 × 500 m. As shown in Figure. 7, the server node (vehicle node car1) which is connected to RSU1, transmits the information to the clients (the vehicle nodes car2 and car3) covered by the entities RSU2 and RSU4 respectively.

We detail the characteristics of our network traffic in Table.2. Depending on the frequency of the RSSI signal received, the vehicle nodes can select the connection point to the network.

We simulate, in the second phase of an area of 2 × 2 km, an overload of the entity RSU1. We consider that the vehicle

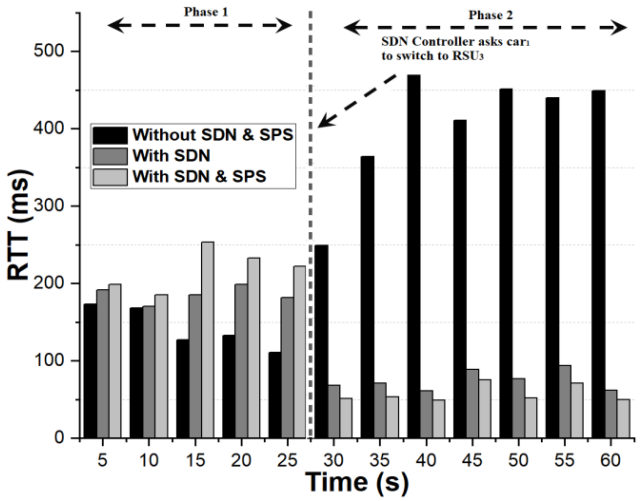

FIGURE 9. Round Trip Time (RTT).

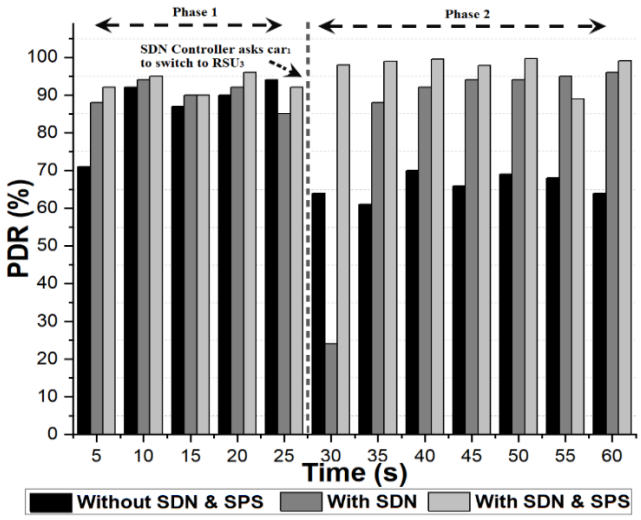

FIGURE 10. Packet Delivery Ratio (PDR).

node car1 is initially attached to RSU1 and that the overload of the RSU1 entity is anticipated by the SDN controller.

The idea is to change the state of vehicle node car1 and become attached to RSU3. As shown in Figure. 8, to support this state change new rules must be implemented in the RSU entities.

B. RESULTS AND ANALYSIS

Two metrics are considered in the first assessments:

- RTT (Round Trip Time): It represents the time required for a round trip of a packet from a given source to a given destination.
- PDR (Packet Delivery Ratio): It characterizes transmission reliability. It represents the ratio of the number of successfully routed packets to the total number of packets transmitted by the source.

Figures. 9 and 10 show the communication performance results between the car1 and car2 vehicle nodes with and without the application of control, and with and without the presence of our security and privacy scheme (SPS). They show respectively the Round Trip Time and the Packet Delivery Ratio.

We can conclude that the performance of the network deteriorates when the vehicle node car1 is attached to the entity RSU1 and the latter is overloaded. The Packet Delivery Ratio decreases by 30% and the Round Trip Time decreases from 111 ms to 449 ms. However, it can be seen that the performance of the network is improved when SDN triggers the change of the RSU entity (attached to the vehicle node car1). Such as we notice that the average RTT is lowered by 68 ms and that the PDR remains around 94%. We also notice with the integration of the SPS that the performance of the network is improved, the average RTT is reduced by 51 ms and the PDR persists around 99%.

We also notice that the PDR drops to 18% with the forwarding action between RSUs which has a network performance cost. Nevertheless, this loss can be compensated by the significant gain in performance in transmission, which can be used to catch up with certain delays and losses related to the change of RSU. This fully motivates the consideration of control via SDN and SPS in a very dynamic VANET environment.

The consideration of the SDN paradigm as a key principle in the design of new vehicular network architectures poses again the challenge concerning the placement of controllers. Finding a good investment strategy is essential to guarantee the best performance, especially when it comes to supporting ITS services with very strict requirements. The first element of this strategy is to consider the possibility that the RSU entities can host the controllers [40]. The RSU entities (chosen as controllers) have limited resources (processing, storage), which restricts their ability to manage many nodes simultaneously, compared to controllers usually installed in data centers. In our simulations, we consider the network traffic proposed in [40] to show the impact of the SDN controller and our security and privacy scheme on the performance of the studied VANET network.

We consider three scenarios with different numbers and locations of vehicle nodes such as 50, 100, and 200. Mininet-WiFi's base controller operates in hop-by-hop mode, which means that each RSU entity that is part of a data path, in turn, asks the controller which routing rule to install via the Packet-In/Packet-out message exchange. Two metrics are evaluated:

- Overhead: This reflects all messages generated by all vehicle nodes and RSUs, mainly during the routing rule installation process.
- Flow Setup Time (FST): this is the difference between the time when a vehicle node or RSU sends a Packet-In type message to the controller and the moment when it receives its corresponding response message, Packet-Out type (flow instantiation rule).

Figures. 11 (a) and (b) show respectively the overhead and the average FST as a function of the maximum number of jumps (tolerated by the placement strategy) and the number

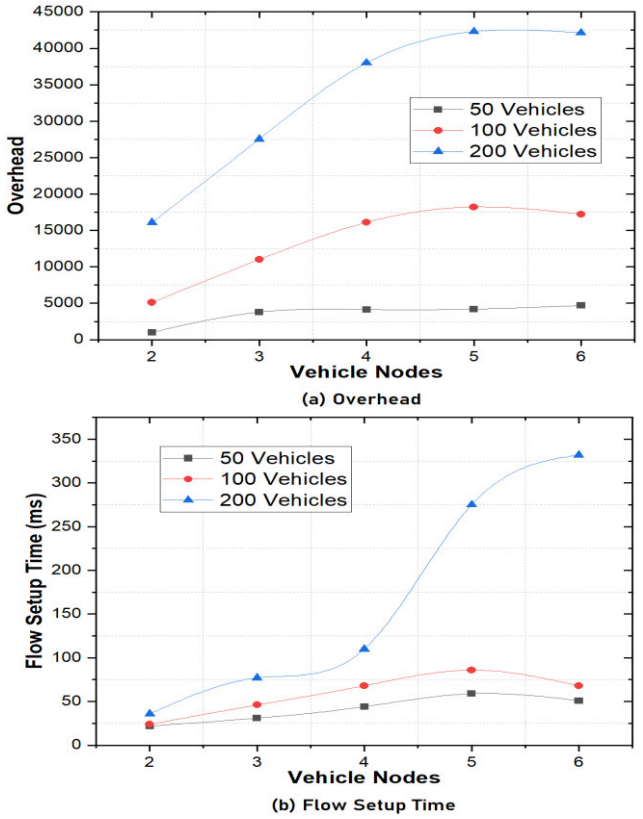

FIGURE 11. Placement performance as a function of controller load and coverage.

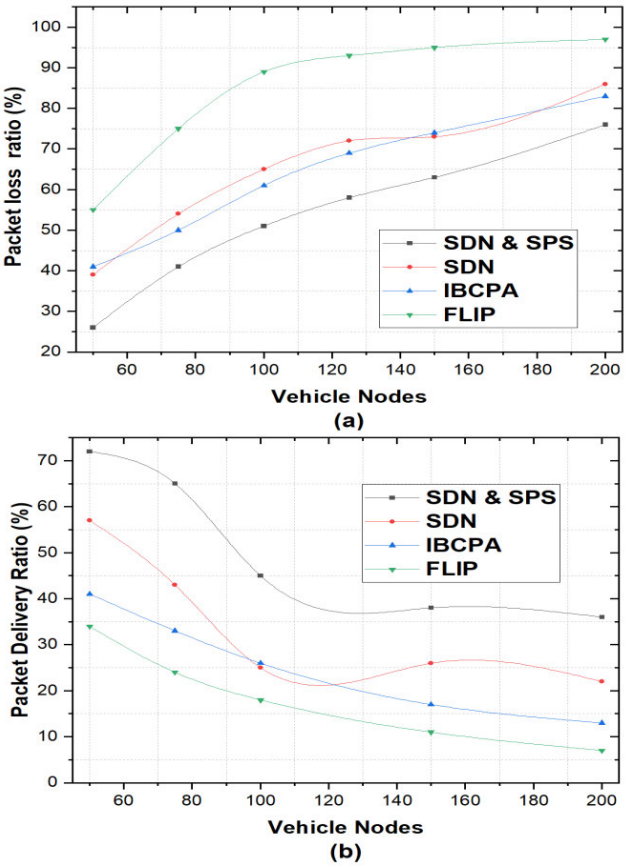

FIGURE 12. Packet Loss Ratio vs. VANET network size and (b) Packet Delivery Ratio vs VANET network size.

of vehicles. As expected, the overhead and the FST increase according to the maximum number of hops between the controller and the vehicles, for the three, examined scenarios. The increase in overhead mainly depends on the number of packet-in messages generated. The more vehicles we have, the more traffic there will be generated and therefore more overhead. On the other hand, the increase in controller coverage implies the dispersion of vehicles in the considered topology. This implies that the data paths include more intermediate nodes and therefore the generation of a significant number of Packet-In messages. It can be seen that the increase in Overhead and FST is more significant in the scenario of 200 vehicles. The simulation tool does not allow us to consider a larger number of vehicles to more accurately assess the performance of OpenFlow sessions between vehicles and the controller. Nevertheless, the evaluations reveal trends, in particular, the significant increase in traffic control and interaction times between controller and vehicles as soon as the number of vehicles is substantial. This increase in delay is due to the increased load on the controller and the impact of the increased load on the vehicle-to-RSU wireless links. These links represent an integral part of the data path connecting the controllers to the vehicles. Thus, an efficient placement strategy must consider that the majority of controlled nodes (vehicles) are close to their controller (reduced coverage) and limit the number of vehicles associated with a single controller.

With a different number of vehicle nodes and with the two schemes considered, we illustrate in Figure. 12 (a) the Packet Loss Rate (PLR). We can notice in this Figure that with an increase in network traffic, the PLR also increases. With a scenario of 100 vehicle nodes, the rate drops from 39 to 86% applying only the first confidentiality and security scheme. On the other hand, with the same number of vehicle nodes, it decreases from 26 to 73% if we also incorporate the SDN control.

Therefore, the PLR becomes weaker, reducing the number of vehicle nodes in our traffic VANET. By comparing it with the FLIP scheme [76], the two proposed schemes offer a lower PLR. Also, with the same load conditions, the two proposed schemes (SDN) and (SPS) are better in terms of PLR compared to the Identity-Based Conditional Privacy-Preserving Authentication Scheme (IBCPA) [77].

With a different number of vehicle nodes and with the two schemes considered for VANET networks, we illustrate in Figure. 12 (b) is the Message Delivery Report (PDR) but compare it in this case with the two schemes IBCPA and FLIP. By applying SDN and SPS, we can notice that the MDR goes from 15% to 22% of the MDR value. We can also notice the difference in MDR value by applying only SDN with the same load conditions. At the same number of vehicle nodes, the combination of our two models gives better results than

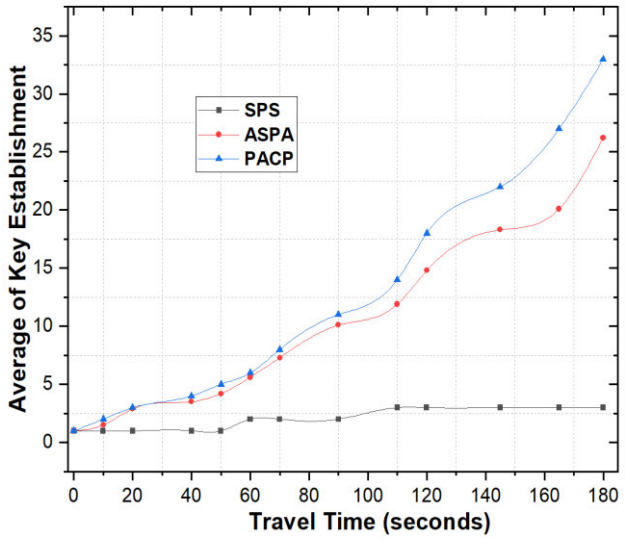

FIGURE 13. The average number of key establishments.

FLIP and IBCPA. However, SDN & SPS produces a better PDR with 15% more than SDN alone, in the case of a scenario of vehicles at 50 knots or less. We can conclude that the SPS scheme is well suited for heavy traffic and an application that requires reliable and secure message delivery in the VANET network.

To communicate with each other, the vehicle nodes of each group must use the group leader key. Additionally, vehicle nodes must exchange keys with each RSU individually. Vehicle nodes exclusively use the group key shared between them with our SPS scheme. Our travel strategy is assumed to be free (direction and distance) for all vehicle nodes in our simulations. Each group of VANET traffic is covered by four RSUs.

We can notice in Figure. 13 that the average number of key establishments in ASPA (Advanced Strong Pseudonym-based Authentication) [78] and in PACP (Pseudonym Authentication Based Conditional Confidentiality Protocol) [79] becomes more important when the groups are not used. Note that when the beams are not brought into play within the 180 s time interval, 13 independent keys have been transmitted.

VI. CONCLUSION

The contributions proposed in this paper aim at the development of a new security concept of vehicular network programmable via SDN. For the first contribution, we defined vehicular network architecture based on the SDN paradigm. We also presented the proposed approach for placing SDN controllers in the network. This study focused mainly on the first-level controllers of the defined architecture. The proposed model is based on a linear formulation. Our industry-leading approach is to adjust placement based on traffic fluctuations. The combination of the properties of the hybridization of vehicular networks and the SDN paradigm makes the success of the studied architecture. We were also interested in the controller placement is very critical and must be done carefully to take advantage of the benefits of centralized control without impacting the overall performance of the network. To further secure VANET networks, we have also come up with a second intelligent packet protection scheme (SPS). We evaluated the behavior of SDN and SPS in terms of message loss rate, packet delivery rate, and delay reduction. This evaluation allowed us to demonstrate that SDN and SPS are capable of generating many vehicle communications while maintaining the expected properties of the network, particularly in terms of security and confidentiality. However, we did not evaluate the real-time performance of the entire system.

Several perspectives are possible such as the operating mode of data exchange between the different actors of this system, the definition of the view of the network to be shared, and how it will be shared, which can constitute a first perspective of architectural order. The definition of an approach taking into account the mobility constraints of vehicular nodes in a vehicular environment represents a second architectural perspective to be explored.

Furthermore, taking a dynamic approach to placing SDN controllers is very promising. An analysis of the processing time for capturing messages, extracting attributes and registering them in the ontology, analyzing the window, and generating the report in the event of an anomaly would make it possible to assess the hardware needs of the device for its integration into the vehicle.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education and Qassim University, Saudi Arabia for funding this research work through the project number (QU-IF-4-4-1-25472).

REFERENCES

[1] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the Internet of Vehicles," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108558.
[2] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1145–1168, 2020.
[3] M. Alawi, R. Alsaqour, M. Ismail, E. Sundararajan, and M. Abdelhaq, "Vehicular Wi-Fi offloading in heterogeneous vehicular networks: Techniques and challenges," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 560–579, Jun. 2018.
[4] B. Chen, L. Wu, N. Kumar, K.-K.-R. Choo, and D. He, "Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1753–1764, Oct. 2021.
[5] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–25, Jan. 2020.
[6] W. Drira, K. Ahn, H. Rakha, and F. Filali, "Development and testing of a 3G/LTE adaptive data collection system in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 1, pp. 240–249, Jan. 2016.
[7] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, *Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges*, vol. 50. Cham, Switzerland: Springer, 2012, pp. 217–241.
[8] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, Vol. 19, no. 16, p. 3589, 2019, doi: 10.3390/s19163589.
[9] L. Xie and S. Zhu, "Message dropping attacks in overlay networks: Attack detection and attacker identification," *ACM Trans. Privacy Secur.*, vol. 11, no. 3, pp. 1–30, 2008.

[10] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100458.

[11] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined VANET: Architecture and services," in *Proc. 13th Annu. Medit. Ad Hoc Netw. Workshop (MED-HOC-NET)*, Jun. 2014, pp. 103–110.

[12] D. K. N. Venkatramana, S. B. Srikantaiah, and J. Moodabidri, "SCGRP: SDN-enabled connectivity-aware geographical routing protocol of VANETs for urban environment," *IET Netw.*, vol. 6, no. 5, pp. 102–111, Sep. 2017.

[13] X. Ji, H. Yu, G. Fan, and W. Fu, "SDGR: An SDN-based geographic routing protocol for VANET," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 276–281.

[14] X. Zhang, H. Zhong, C. Fan, I. Bolodurina, and J. Cui, "CBACS: A privacy-preserving and efficient cache-based access control scheme for software defined vehicular networks," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1930–1945, 2022, doi: 10.1109/TIFS.2022.3174389.

[15] Y.-C. Liu, C. Chen, and S. Chakraborty, "A software defined network architecture for GeoBroadcast in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 6559–6564.

[16] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 1202–1207.

[17] A. Kazmi, M. A. Khan, and M. U. Akram, "DeVANET: Decentralized software-defined VANET architecture," in *Proc. IEEE Int. Conf. Cloud Eng. Workshop (IC2EW)*, Apr. 2016, pp. 42–47.

[18] A. Glena, "Software defined network based VANET," *Int. J. Sci. Bus.*, vol. 5, no. 3, pp. 83–91, 2021.

[19] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, and M. Qiu, "A scalable and quick-response software defined vehicular network assisted by mobile edge computing," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 94–100, Jul. 2017.

[20] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[21] L. Liang, H. Ye, and G. Y. Li, "Toward intelligent vehicular networks: A machine learning framework," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 124–135, Feb. 2019.

[22] D. Zhang, F. R. Yu, and R. Yang, "Software-defined vehicular networks with trust management: A deep reinforcement learning approach," *IEEE Trans. Intell. Transp.*, vol. 23, no. 2, pp. 1400–1414, Feb. 2022, doi: 10.1109/TITS.2020.3025684.

[23] S. K. Tayyaba, H. A. Khattak, A. Almogren, M. A. Shah, I. U. Din, I. Alkhalifa, and M. Guizani, "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020.

[24] A. A. Z. Ibrahim, F. Hashim, A. Sali, N. K. Noordin, and S. M. E. Fadul, "A multi-objective routing mechanism for energy management optimization in SDN multi-control architecture," *IEEE Access*, vol. 10, pp. 20312–20327, 2022, doi: 10.1109/ACCESS.2022.3149795.

[25] H. Zhong, J. Fan, J. Cui, Y. Xu, and L. Liu, "Assessing profit of prediction for SDN controllers load balancing," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107991.

[26] D. Kreutz, J. Yu, F. M. V. Ramos, and P. Esteves-Verissimo, "ANCHOR: Logically centralized security for software-defined networks," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–36, May 2019.

[27] A. George, A. Ravindran, M. Mendieta, and H. Tabkhi, "Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge," *IEEE Access*, vol. 9, pp. 21457–21473, 2021, doi: 10.1109/ACCESS.2021.3055775.

[28] B. Heller, R. Sherwood, and N. M. Keown, "The controller placement problem," in *Proc. HotSDN*, vol. 12. New York, NY, USA, 2012, pp. 7–12.

[29] G. Wang, Y. Zhao, J. Huang, Q. Duan, and J. Li, "A K-means-based network partition algorithm for controller placement in software defined network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[30] Y. Hu, T. Luo, W. Wang, and C. Deng, "On the load balanced controller placement problem in software defined networks," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Oct. 2016, pp. 2430–2434.

[31] B. Isong, R. R. S. Molose, A. M. Abu-Mahfouz, and N. Dladlu, "Comprehensive review of SDN controller placement strategies," *IEEE Access*, vol. 8, pp. 170070–170092, 2020.

[32] D. Hock, M. Hartmann, S. Gebert, M. Jarschel, T. Zinner, and P. Tran-Gia, "Pareto-optimal resilient controller placement in SDN-based core networks," in *Proc. 25th Int. Teletraffic Congr. (ITC)*, Sep. 2013, pp. 1–9.

[33] S. Lange, "Heuristic approaches to the controller placement problem in large scale SDN networks," *IEEE Trans. Netw. Service Manag.*, vol. 12, no. 1, pp. 4–17, Mar. 2015.

[34] M. Cello, Y. Xu, A. Walid, G. Wilfong, H. J. Chao, and M. Marchese, "BalCon: A distributed elastic SDN control via efficient switch migration," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2017, pp. 40–50.

[35] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, "Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects," *IEEE Access*, vol. 10, pp. 70850–70901, 2022, doi: 10.1109/ACCESS.2022.3188311.

[36] M. A. Saleem, Z. Shijie, and A. Sharif, "Data transmission using IoT in vehicular ad-hoc networks in smart city congestion," *Mobile Netw. Appl.*, vol. 24, no. 1, pp. 248–258, Feb. 2019.

[37] B. Mao, F. Tang, Z. M. Fadlullah, and N. Kato, "An intelligent route computation approach based on real-time deep learning strategy for software defined communication systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1554–1565, Jul. 2021.

[38] A. Dvir, Y. Haddad, and A. Zilberman, "Wireless controller placement problem," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–4.

[39] M. J. Abdel-Rahman, E. A. Mazied, K. Teague, A. B. MacKenzie, and S. F. Midkiff, "Robust controller placement and assignment in software-defined cellular networks," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–9.

[40] K. S. K. Liyanage, M. Ma, and P. H. J. Chong, "Controller placement optimization in hierarchical distributed software defined vehicular networks," *Comput. Netw.*, vol. 135, pp. 226–239, Apr. 2018.

[41] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.

[42] P. Li, T. Miyazaki, K. Wang, S. Guo, and W. Zhuang, "Vehicle-assist resilient information and network system for disaster management," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 438–448, Jul. 2017.

[43] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.

[44] B. Greenshields, J. Bibbins, W. Channing, and H. Miller, "A study of traffic capacity," in *Highway Research Board Proceedings*, vol. 1935. Montreal, QC, Canada: National Research Council (USA), Highway Research Board, 1935.

[45] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A deep learning based intrusion detection method in VANET," in *Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2019, pp. 288–293.

[46] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," in *IEEE Access*, vol. 10, pp. 1893–1904, 2022, doi: 10.1109/ACCESS.2021.3136706.

[47] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, 2012.

[48] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[49] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842.

[50] S. M. A. Al Mamun and J. Valimaki, "Anomaly detection and classification in cellular networks using automatic labeling technique for applying supervised learning," *Proc. Comput. Sci.*, vol. 140, pp. 186–195, Jan. 2018.

[51] V. Singh and K. Mahajan, "VANET and its security Issues—A review," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 10, pp. 59–64, 2016.

[52] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: Towards security issues review," in *Proc. IEEE 5th Int. Symp. Telecommun. Technol. (ISTT)*, Nov. 2020, pp. 151–156, doi: 10.1109/ISTT50966.2020.9279375.

[53] K. Rabah, "Theory and implementation of elliptic curve cryptography," *J. Appl. Sci.*, vol. 5, no. 4, pp. 604–633, Mar. 2005.
[54] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779, doi: 10.1016/j.jisa.2021.102z779.
[55] Y.-M. Tseng, J.-K. Jan, and H.-Y. Chien, "Digital signature with message recovery using self-certified public keys and its variants," *Appl. Math. Comput.*, vol. 136, nos. 2–3, pp. 203–214, Mar. 2003.
[56] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779, doi: 10.1016/j.jisa.2021.102779.
[57] B. Alaya, "Efficient privacy-preservation scheme for securing urban P2P VANET networks," *Egyptian Informat. J.*, vol. 22, no. 3, pp. 317–328, Sep. 2021, doi: 10.1016/j.eij.2020.12.002.
[58] K. Assafra, B. Alaya, and M. Abid, "Privacy preservation and security management in VANET based to software defined network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 96–101, doi: 10.1109/WCNC51071.2022.9771705.
[59] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522–121531, 2021, doi: 10.1109/ACCESS.2021.3109264.
[60] I. Toshiyuki, M. Nguyen, and K. Tanaka, "Proxy re-encryption in a stronger security model extended from CT-RSA2012," in *Proc. Cryptographers' Track RSA Conf.*, 2013, pp. 277–292.
[61] M. A. Shawky, A. Jabbar, M. Usman, M. Imran, Q. H. Abbasi, S. Ansari, and A. Taha, "Efficient blockchain-based group key distribution for secure authentication in VANETs," *IEEE Netw. Lett.*, vol. 5, no. 1, pp. 64–68, Mar. 2023, doi: 10.1109/LNET.2023.3234491.
[62] K. A. Awan, I. U. Din, and A. Almogren, "A blockchain-assisted trusted clustering mechanism for IoT-enabled smart transportation system," *Sustainability*, vol. 14, no. 22, Nov. 2022, Art. no. 14889, doi: 10.3390/su142214889.
[63] Y. Zhou, L. Cao, Z. Qiao, Z. Xia, B. Yang, M. Zhang, and W. Zhang, "An efficient identity authentication scheme with dynamic anonymity for VANETs," *IEEE Internet Things J.*, early access, Jan. 13, 2023, doi: 10.1109/JIOT.2023.3236699.
[64] D. Grewe, M. Wagner, M. Arumaithurai, I. Psaras, and D. Kutscher, "Information-centric mobile edge computing for connected vehicle environments: Challenges and research directions," in *Proc. Workshop Mobile Edge Commun.*, Aug. 2017, pp. 7–12.
[65] M. Wegner, T. Schwarz, and L. Wolf, "Connectivity maps for V2I communication via ETSI ITS-G5," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2018, pp. 1–8.
[66] A. Rullo, D. Midi, E. Serra, and E. Bertino, "Pareto optimal security resource allocation for Internet of Things," *ACM Trans. Privacy Secur.*, vol. 20, no. 4, pp. 1–30, Nov. 2017.
[67] R. Brendha and V. S. J. Prakash, "A survey on routing protocols for vehicular ad hoc networks," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–7.
[68] K. Ahed, M. Benamar, A. A. Lahcen, and R. E. Ouazzani, "Forwarding strategies in vehicular named data networks: A survey," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 5, pp. 1819–1835, May 2022.
[69] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Comput. Sci. Rev.*, vol. 36, May 2020, Art. no. 100235, doi: 10.1016/j.cosrev.2020.100235.
[70] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proc. NDSS*, 2000, pp. 143–154. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/042.pdf
[71] P. Agarwal, "Secure node communication with cryptographic algorithm in vehicular ad hoc networks," *Int. J. Adv. Sci. Technol.*, vol. 109, pp. 1–12, Dec. 2017.
[72] R. Lu, X. Lin, X. Liang, and X. Shen, "Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in VANET," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Dec. 2010, pp. 1–5.
[73] C. Kalaiarasy and N. Sreenath, "An incentive-based co-operation motivating pseudonym changing strategy for privacy preservation in mixed zones in vehicular networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1510–1520, Jan. 2022.
[74] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[75] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, "Mininet-WiFi: Emulating software-defined wireless networks," in *Proc. 11th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2015, pp. 384–389.
[76] H. Bartlett, E. Dawson, H. Qahur Al Mahri, M. I. Salam, L. Simpson, and K. K.-H. Wong, "Random fault attacks on a class of stream ciphers," *Secur. Commun. Netw.*, vol. 2019, pp. 1–12, Jul. 2019.
[77] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," *Symmetry*, vol. 12, no. 10, p. 1687, Oct. 2020.
[78] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PloS ONE*, vol. 15, no. 2, pp. 1–19, 2020, doi: 10.1371/journal.pone.0228319.
[79] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din, and G. Ali, "ASPA: Advanced strong pseudonym based authentication in intelligent transport system," *PLoS ONE*, vol. 14, no. 8, Aug. 2019, Art. no. e0221213.

BECHIR ALAYA was born in Tunisia, in November 1980. He received the master's degree in computer science from Le Havre University, France, in June 2007, and the joint Ph.D. degree in computer science from Le Havre University and Sfax University, Tunisia, in October 2012. His master's thesis had been concentrated on QoS management in distributed multimedia systems. His Ph.D. research work had been concentrated on proposing some QoS management techniques to resolve the congestion problems in distributed multimedia systems, on which he has published multiple publications in prestigious international journals and conferences. He is currently an Assistant Professor with the College of Science and Technology of Gabes, ISSATG, Gabes University, Tunisia, in September 2012, and has been with the Department of Management Information Systems (MIS), College of Business & Economics (CBE), Qassim University, Saudi Arabia, since September 2014. His research interests include real-time databases systems, real-time nested transactions, distributed multimedia systems, video streaming and QoS management in multimedia networks, vehicular *ad-hoc* networks (VANET), VANET security, fuzzy systems, clustering, and job shop.

LAMAA SELLAMI received the master's degree in artificial intelligence techniques and the Ph.D. degree in electrical engineering from Gabes University, Tunisia, in June 2007 and 2016, respectively. Since 2017, she has been an Assistant Professor with the MIS Department, CBE, Qassim University, Saudi Arabia. Her research interest includes vehicular *ad-hoc* networks (VANET). Her current research interests include Internet-of-Things (IoT) security, especially in using and adopting clustering techniques in the VANET environment, fuzzy logic, and fuzzy regression.