IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 14 June 2024, accepted 4 July 2024, date of publication 8 July 2024, date of current version 13 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3425053

RESEARCH ARTICLE

Authentication in QoS Aware VANET: An Approach Based on Enhanced Digital Certificates

MOUNA GARAI[1], MAHA SLITI[2,3], MANEL MRABET[4], NOUREDDINE BOUDRIGA[5], AND LASSAAD BEN AMMAR[4]

[1]Higher Institute of Technological Studies of Medenine, Medenine 4100, Tunisia
[2]LR11TIC04, Communication Networks and Security Research Laboratory, Higher School of Communication of Tunis (SUP'COM), University of Carthage, Ariana 2083, Tunisia
[3]LR11TIC02, Green and Smart Communication Systems Research Laboratory, Higher School of Communication of Tunis (SUP'COM), University of Carthage, Ariana 2083, Tunisia
[4]Department of Computer Sciences, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[5]Higher School of Communication of Tunis (SUP'COM), University of Carthage, Ariana 2083, Tunisia

Corresponding author: Manel Mrabet (M.benrashed@psau.edu.sa)

This study is supported via funding from Prince sattam bin Abdulaziz University project number (PSAU/2024/R/1445).

ABSTRACT Vehicular Ad-hoc Networks (VANETs) indeed have significant potential to enhance transportation efficiency, accident prevention, and overall comfort. They enable communication between vehicles and road infrastructure, facilitating the exchange of entertainment and traffic information. This capability can lead to safer and more efficient transportation systems while improving the overall experience for drivers and passengers. The challenging and critical security requirements in VANETs, such as access management, authentication, and privacy protection, are essential for achieving the objectives of vehicle-to-infrastructure (V2I) and intervehicle (I2V) communications. These security measures ensure the integrity, confidentiality, and availability of communication channels, thereby enhancing transportation efficiency, accident prevention, and overall comfort within VANETs. In this study, we investigate the concerns of secure access control, authentication, and privacy protection in VANETs. In response to these challenges, we propose automobile authentication methods. This protocol is built on a toll-based certificate management system utilizing RFID tags and readers deployed on automobiles and toll booths. Additionally, we introduce a vehicular mobility management method and a VANET node attachment strategy that considers quality of service (QoS) requirements. This comprehensive approach addresses key security and operational aspects of VANETs.

INDEX TERMS Vehicular ad hoc network, quality of service, entity authentication, access control, radio frequency identification, digital certificates.

I. INTRODUCTION

VANETs (Vehicular Ad Hoc Networks) are critical components of Intelligent Transportation Systems. VANET development has garnered significant attention and research effort from both the academic community and automobile manufacturers in recent years [1]. The development of VANETs has made it possible to implement numerous value-added services that enhance transportation comfort and safety. It is essential that these services adhere to a constrained quality of service (QoS) specification, which may include controlled jitter and minimized latency of the transmitted packets. The highly dynamic topology of VANETs, on the other hand, causes a number of major technical problems that make them more vulnerable to attacks in areas like routing consistency, resource availability, and communication continuity.

Because of the high mobility of vehicles, the variety of wireless channel conditions, and the scarcity of wireless resources, QoS provision was undoubtedly a problematic

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

issue. Conversely, the exploitation of confidential information pertaining to the vehicle compromises privacy and decreases the utility of the services provided by VANETs. The mobile vehicle's location may be tracked, sent messages from the automobiles might be collected and used to deduce critical data, and false data could be added to the beacons that are exchanged. Hence, there is a pressing need for methodologies that enhance security and privacy in order to facilitate message authentication, distinguish legitimate automobiles, and isolate the communication of malicious vehicles.

Two notable technologies that have achieved substantial progress and can be advantageous when integrated into VANETs are radio frequency identification (RFID) and digital certification. RFID refers to the utilization of radio waves for the purpose of automatically detecting and identifying adjacent objects. The process involves attaching tags to things using a transmitter, also known as a reader, that can emit information packets, including the tag's identity, when it comes into contact with a tag. RFID technology is currently utilized across various industries, such as transportation and healthcare, to provide automated support for daily operations, owing to its numerous advantages. Although RFID integration has many advantages, there are a number of barriers to its widespread use in mobile vehicle identification. Three significant concerns can be identified among the principal drawbacks: The first issue concerns the security of the tags, which are vulnerable to a variety of physical attacks. The necessity for privacy regarding the gathered data is the second concern, given that the observations captured on tags may be exploited to compromise privacy. The third factor is the accuracy of the data gathered from the tags. In fact, this collected data is too small to allow the special and temporal dimensions of tracking moving cars on a highway.

Digital certification, on the other hand, refers to the process of establishing a digital certificate and using it to instantly identify the certificate's owner. Ensuring a robust correlation between the proprietor's identity and the public key displayed on the certificate, as well as a confidential private key retained by the proprietor, is the objective of the creation procedure. The generating technique includes a registration task that checks the identification and specifies the amount of trust that should be assigned to the created certificate in order to offer robust authentication. When attempting to integrate digital certification into transportation systems, several challenges must be surmounted. incorporating the subsequent:

- Lack of attributes: Beyond the scope of identity verification, digital certificates can store additional data. Indeed, these entities may contain information that aids the service they provide or divulge details pertaining to the holder's status. The information may be appended to attributes that are no longer commonly utilized or incorporated into digital certificates. Nevertheless, the inclusion of such information would likely require a greater frequency of certificate issuance and revocation.
- Mobility and storage: As mobile certificate holders frequently access services from a variety of locations (e.g., a toll booth along the highway), certificate mobility and, consequently, certificate storage are critical. This gives rise to two issues that require resolution: (a) the method by which users can load and utilize their digital certificates and keys across multiple access points; and (b) the protocol by which users should load and utilize certificates and keys on shared computers.
- False trust: Digital certificates are susceptible to false trust from both users and service providers. A public key infrastructure (PKI) is implemented to ensure that all certificates issued by PKI-affiliated authorities are supported by a root authority or a widely recognized authority and that a relationship of trust is intrinsically established among these authorities in order to address this concern.

Additional challenges may arise with the certification sub-processes when they are implemented in VANETs. In order to access a service (such as a toll booth located at the entrance to a highway), a vehicle might solely be required to undergo the generation procedure. This could request that the registration subprocess make use of the vehicle's physical characteristics in order to facilitate strong authentication. An additional issue that arises is the manner in which registration ought to be executed, given the evident lack of suitability of conventional registration processes for VANETs.

In this article, we propose a QoS-aware VANET authentication approach, certification method, and access control strategy in order to address important aspects of security, privacy, and service quality in vehicular networks.

1) The QoS-aware VANET authentication approach integrates RFID technology and certification processes. It is a promising direction for enhancing security and quality of service in vehicular networks. In fact, the inclusion of authentication mechanisms at various locations along transportation routes, such as toll stations, is a practical strategy to ensure secure communication and access control for vehicles.
2) Using the RFID technology, the node locations along transportation routes used to generate a temporary identity and a performing a temporary certification. That's why a revocation of certification is proposed. we provide an **authentication method** that protects vehicle privacy and inhibits the transmission of the global vehicle identity within the vehicular network. In order to thwart various assaults and ensure the delivery of added value, services, a secure routing protocol, and safe traffic exchange are offered based on the produced certificates.
3) Certification method is implemented to safeguard user privacy, circumvent diverse threats, and enable real-time certificate issuance and validation through the application of distinct patterns to issued certificates.

Numerous attributes are appended to the certificates in order to bolster the authentication process's reliability. For the purpose of ensuring resilience, we recommend integrating the authentication process into a tree-based VANET architecture.

4) Access control strategy is proposed. in witch the access of nodes in the tree considers the quality of service requirements. in fact, a secure tree-based communication architecture is first proposed, enabling the quick connection of mobile vehicles. In this design, a vehicle only needs to listen to the messages broadcast by linked neighbors and choose the route delivering the best QoS to gain access to the network. The latter contribution has been based on the **QoS model** we have developed in [2].

This paper's remaining sections are arranged as follows:. The most pertinent works are compiled in Section II, along with a discussion of the limitations of the current fixes. In order to enable QoS-aware service access, Section III outlines the tree-based network architecture and creates a QoS model. It also describes mobility management and the QoS-aware vehicle attachment process. The functions of managing digital certificates for vehicles are explained in Section IV. The proposed VANET architecture's vehicle authentication system is explained in Section V. The performance analysis of the authentication protocol and QoS model is covered in Section VI, along with the development of numerical experiments. This paper is finally concluded in Section VII.

II. STATE OF THE ART

The development of VANET has created a wide range of opportunities for strong and alluring services that can provide security and effectiveness for the comfort of drivers and other road users. In fact, vehicles can include wireless communication capabilities, embedded sensors, processing tools, and the ability to access services and relay data. Data communication and service design in VANETs are now faced with additional difficulties due to the high mobility the vehicles can attain and the large amount of data they can share. The VANETs' highly dynamic topology, their uneven communication connectivity, and their wide range of application QoS requirements actually present challenging problems to solve ([1] and [2]).

Two main problems must be solved for VANET's accessible services to operate more efficiently. First, in order to find routes that meet the various QoS requirements of the services offered over them, vehicular networks should first use QoS routing protocols. Second, in order to prevent a wide range of attacks that could reduce the quality of service (QoS) offered by the network and increase the attack victims' resource consumption, the security of the routing process and access control should be addressed. We review the efforts made to address these challenges in the sections that follow.

A. SECURITY ISSUES IN VEHICULAR AD HOC NETWORKS

The development of VANET (Vehicular Ad Hoc Network) has led to the provision of various services that enhance road user safety, comfort, and traffic efficiency [3]. However, security and privacy concerns pose significant challenges in this open-access environment and may impact the success of VANETs when widely implemented [4]. Several research studies have examined the security challenges and privacy-preserving techniques for VANETs [4], [5], [6], [7].

One study classified security threats and proposed authentication methods and privacy-preserving techniques [4]. Another study focused on grouping VANET security problems from a cryptographic perspective and evaluated different cryptographic schemes for VANETs [5]. Routing protocols and privacy-preserving authentication schemes were also presented in separate studies [6], [7].

Furthermore, the use of digital certificates in VANETs has been addressed, particularly the challenge of revocation. Proposed solutions have not fully resolved this issue, and the unavailability or unreachability of roadside infrastructure poses additional challenges [7]. Several protocols, such as Ariadne, SAODV, SEAD, ARAN, and ECDSA, have been proposed for safe routing in automotive ad hoc networks, but each protocol focuses on a specific security function and is vulnerable to routing attacks [8].

To address these challenges, researchers have developed various authentication protocols, such as the ZK authentication protocol and a cluster-based enhanced authentication and communication protocol [9], [10]. Additionally, access control mechanisms, routing mechanisms, and authentication schemes have been proposed to improve security while minimizing delay, overhead, and energy consumption [10], [11], [12].

Overall, these studies highlight the security and privacy concerns in VANETs and propose various solutions to address them, including authentication methods, privacy-preserving techniques, routing protocols, and access control mechanisms.

B. QOS ISSUES IN VEHICULAR AD HOC NETWORKS

The authors of [13] introduced a channel access scheme called EDFCSMA for VANETs, which demonstrated higher channel utilization compared to other mechanisms. However, it was limited to unidirectional VANETs and did not include multi-hop VANETs or heterogeneous ad hoc networks.

In [14], the authors proposed a secure value-added service scheme for VANETs using undefined signature technique and incorporating multiple security measures. However, they did not disclose QoS metrics for secured communication connections.

A privacy-preserving and secure scheme for value-added VANET applications was proposed in [15], which included anonymous vehicle services and a tracing mechanism to prevent abuse. However, the authors did not establish or assess QoS parameters for value-added applications.

In [16], a secure and privacy-preserving scheme for vehicular communication using identity-based aggregated signatures was proposed, showing improvements in latency and response time. However, QoS parameters critical for the communication protocol were not explored.

The authors of [17] proposed a reliable and secure multi-constrained QoS-aware routing algorithm for VANETs, using the S-AMCQ routing algorithm and the extended VoEG to guarantee message integrity. However, the authentication process was limited to routing control messages and security algorithms may incur costs in terms of bandwidth, response time, and latency.

In [18], an algorithm was devised to minimize authentication bandwidth and latency to defend against network attacks in VANETs.

A dual authentication scheme was suggested in [19] to enhance the security of VANET communication, along with a dual group key management scheme. However, a method to safeguard vehicle location anonymity was not devised.

Other studies on VANET QoS for value-added services include the development of HOQC-MAC protocol [23], a proactive routing protocol based on OLSR [20], analysis of data dissemination strategies [21], and a novel approach for vehicle clustering and routing [22].

The [25] suggests a secured protocol called TT-SHO that combines hybrid chaotic encryption and Tent Tuned Spotted Hyena Optimization (TT-SHO) for routing algorithm in VANETs.

C. RFID-BASED AUTHENTICATION FOR VANET

RFID technology is widely used for object-specific identification, including in the identification of armaments [26]. Various authentication schemes have been proposed for RFID tags in VANETs, such as a certificate revocation status validation scheme [26], an RFID authentication protocol adhering to the EPC-C1G2 standard [27], and an improved authentication scheme based on asymmetric key cryptography [28]. However, these schemes have limitations that need to be addressed, such as the need for security analysis, reducing computational time, and improving the certificate revocation process.

Another proposed authentication scheme for VANETs does not rely on RFID readers but instead relies on trust in a database [29]. However, this scheme lacks an efficient approach for retrieving the secret identification value of the tag, making it vulnerable to attacks.

To ensure secure inter-vehicle and vehicle road-side communications, an authentication framework with conditional privacy preservation and non-repudiation has been proposed [30]. Additionally, an access control system for verifying a vehicle's identity when accessing a restricted area has been proposed [31]. However, these schemes may be affected by adjoining systems that can track the vehicle.

RFID System on Roads (RSR) is seen as an essential platform for future transportation systems, providing unique features such as vehicle lane position management, road traffic information control, and driving behavior analysis [32]. Several vehicular applications based on RSR have been developed to enhance transportation safety and efficiency [33], [34].

In the context of VANETs, there have been several research projects focusing on RFID-based authentication. Three works are described, each with different approaches and objectives [35], [36], [9]. The first work focuses on reducing energy consumption and complexity, the second work uses intelligent agents to manage the authentication process, and the third work adapts the authentication process based on network conditions. All three works aim to enhance the security of RFID-based authentication in VANETs.

D. COMPARISON OF EXISTING APPROACHES

Table 1 shows a comparison between the major features of the described works that interest on QoS and security issues and our approach.

In our paper, we propose a tree-based topology for communication in VANETs, which can offer advantages in terms of scalability and routing efficiency. Moreover, this paper considers multi-hop communication links, which are essential in VANETs due to the dynamic and frequently changing network topology. Besides, it evaluates performance metrics such as throughput, delay, packet loss, and route lifetime, which are critical for assessing the efficiency and reliability of communication in VANET environments. To solve security issues, authentication mechanisms are discussed, including certificate-based authentication and temporary identity solutions, which are crucial for ensuring secure communication and preventing unauthorized access. Also, privacy and confidentiality aspects are addressed, highlighting the importance of protecting sensitive information and ensuring data confidentiality in VANET communications. The proposal for secure tree-based access highlights the importance of access control mechanisms in enhancing security and preventing unauthorized entities from accessing the network.

III. A SECURE VANET ARCHITECTURE

This section presents the proposed network architecture, the suggested QoS model, and the mechanisms for delivering, revoking, and renewing certificates that are suitable for this architecture in order to control the vehicle mobility (vehicular mobility management), establish and maintain connectivity within the network (node attachment). In order to improve clarity and justify the proposed models in VANET architecture, some explanations of technical terms are needed.

1) **The vehicle mobility management:** it a is a term used to describe a collection of techniques and strategies intended to efficiently control vehicle mobility inside a vehicular network. The objective of this technique is to maximize resource allocation, routing,

TABLE 1. Comparison of existing approaches.

	Connection issues		Qos Issues		security issues		Proposed solution
Ref	Connection scheme	Routing Protocol	QoS provision	QoS metrics	Security and Privacy	Security Objective	
[7]	Clustering with star topology	One-hop link	Yes	-Delay - Throughput	No	X	Identification based MAC on Address and vehicle location
[10]	Clustering schemes	cluster-based routing protocol	No	X	Yes	integrity, authenticity, and availability of messages in vehicular communication on a specific cluster	secure cluster-based authentication and communication protocols for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.
[11]	clustering schemes	Clustering-based Routing Protocol	Yes	average end-to-end delay, packet delivery rate, and throughput	Yes	Security and privacy	Novel Trust Aware Clustering-based Routing Protocol (TACR) to address the challenges related to security and reliability in VANET communications with minimum computational costs and delay
[12]	X	X	No	X	Yes	-Privacy - authentication scheme -integrity of data	a security-enhanced, high-performance and energy-efficient authentication scheme with CPP for VANETs.

TABLE 1. ***(Continued.)*** **Comparison of existing approaches.**

[10]	Clustering Schemes	Cluster-based routing protocol	Yes	The end-to-end (E2E) delay and route request and reduces link failure	Yes	authentication scheme	Secure cluster-based authentication and communication protocol
[13]	X	X	Yes	-Channel utilization	Yes	Channel access scheme	
[14]	X	One-hop link with RSU	Yes	Computation overhead	Yes	Authentication and Privacy	Access authorization /Mutual authentication
[15]	Hierarchical technology	Multi-hop links	Yes	-Bandwidth -Delay -Transmission Overhead	Yes	Authentication, Privacy and non-repudiation	Anonymous way/Tracking of malicious nodes / Cryptography
[16]	Clustering	Two-hop away	Yes	-End-to-End delay -Delivery Ratio -Bandwidth	No	X	
[17]	novel method for VANET-based efficient vehicle clustering	routing based on network infrastructure for high-performance smart transportation	Yes	-latency -throughput, -packet delivery ratio	No	X	novel method for VANET-based efficient vehicle clustering and routing based on network infrastructure for high-performance smart transportation.
[20]	Multi-Point Relays (MPRs)	Proactive routing protocol, based on the well known OLSR protocol for the VANET proactive network	Yes	-Throughput -Packet Delivery Ratio -Delay	No	X	Modified Harmony Search Optimization Algorithm

TABLE 1. *(Continued.)* Comparison of existing approaches.

[23]	Clustering: QoS-based CH selection	Quality of Service (QoS)-aware Cluster Head (CH) selection and hybrid cryptography named QoS+	Yes	- End-to-End delay	Yes	Security and privacy	Hybrid cryptography module contains Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) algorithms
[25]	X	shortest path optimization and transmits the chaotic encrypted data in the shortest path by maintaining the Quality of Services (QoS)	Yes	latency, Packet Delivery Ratio (PDR) and Throughput	Yes	Data encryption	Novel secured protocol TT-SHO which integrates the Tent Tuned Spotted Hyena Optimization (TT-SHO) for routing algorithm and Hybrid Chaotic Encryption for secured data transmission.
Our paper	Tree Topology	Multi-hop Links	Yes	- Throughput -Delay - Packet Loss -Route lifetime -Blocking rate	Yes	Authentication -Privacy - Reliability - Confidentiality	Temporary identity / Certificate based authentication / Secure tree based access

and communication in dynamic environments where vehicles travel at different speeds.

2) **The VANET attachment Node:** it is a term that describes the process by which vehicles establish and maintain connectivity within the VANET. To guarantee that only authorized vehicles engage in communication. The essential elements node attachment are dynamic attachment/detachment mechanisms, authentication protocols, and digital certificates.

A. NETWORK ARCHITECTURE

For the sake of simplicity, let's concentrate primarily on the example of automobiles traveling along a network of highways where Road Side Units (RSUs) are irregularly placed in order to reduce the expense associated with installing and maintaining the RSU network. We propose a heterogeneous network design that uses RSUs to connect 4G networks with IEEE 802.11p VANETs. As demonstrated in Fig. 1, groups of vehicles connected to the network are organized into tree topology. The RFID-based toll system is composed of RFID tags at toll booths, RFID readers, and RFID systems in vehicles. In fact, every toll booth is equipped with passive RFID tags on the road surface, storing location data including a random number, lane number, direction of travel, and distance to a reference point. RFID scanners connected to the toll system read tags on every vehicle, while

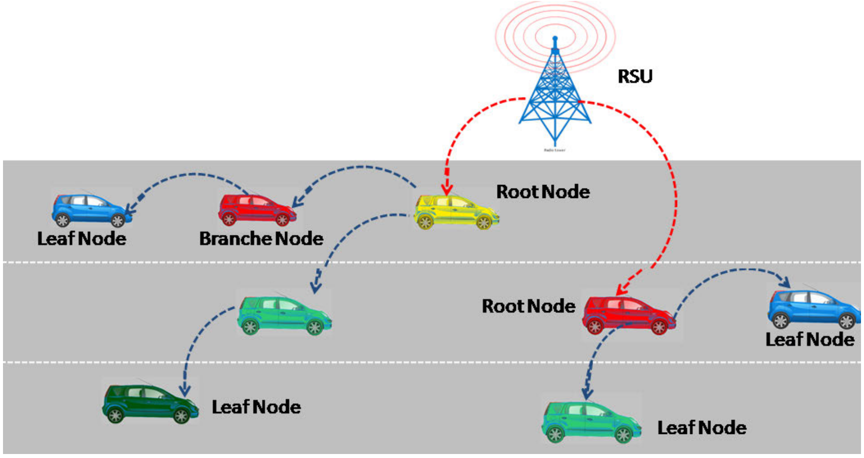

FIGURE 1. VANET architecture.

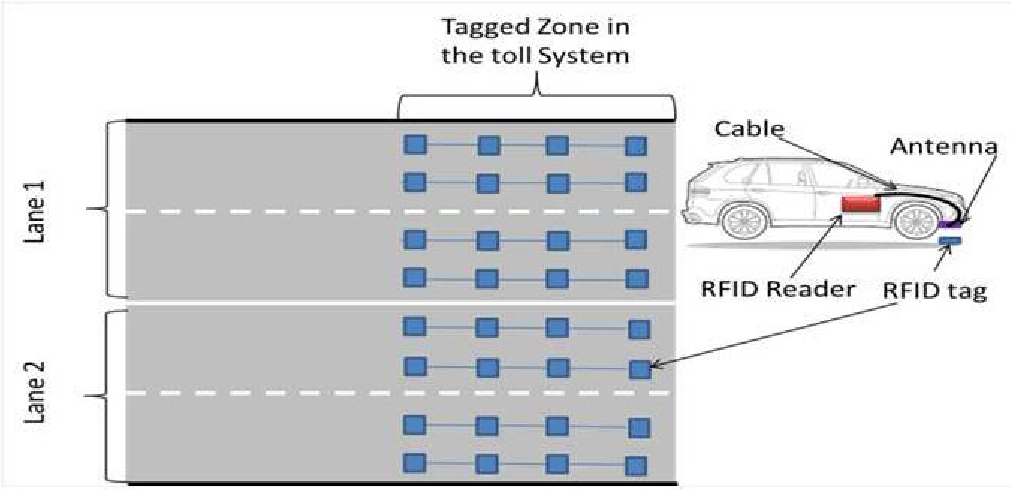

FIGURE 2. Layout of RFID tags and readers in vehicle and tagged zone.

RFID readers in each toll booth prevent tampering. Vehicles are equipped with RFID readers to detect their location in the toll zone and generate authentic data. The RFID system on the road surface and in vehicles is depicted in Fig. 2. Furthermore, We assume that the RFID scanners and roadside RFID tags are connected to a database for authentication, safeguarding vehicle identity against unwanted tracking and modification. In addition, The system includes Local Certification Authorities (LCAs) at toll stations and a Central Trusted Authority (CTA) for RSUs. Digital certificates are used for authentication, and vehicles receive security credentials from LCAs. Finally, several security measures are needed to complete the authentication process. In fact, LCAs gather information from security violations, and the CTA maintains a Certificate Revocation List (CRL) and analyzes security reports from LCAs. Both LCA and CTA are assumed to be robust and hard to manipulate.

The authentication process is established when the vehicle passes through the toll point. The deployed RFID scanners connected to each zone's toll system will read the RFID tags on every vehicle to detect the location of the vehicle and generate authentic data. The toll system's RFID scanners and roadside RFID tags are connected to a database, which can be used to retrieve information that can be used to authenticate the tags.

A lightweight privacy-preserving authentication technique protects the vehicle's identity from unwanted tracking and modification by other cars. Despite the fact that toll stations may employ the tags on the vehicles, digital certificates are used to certify automobiles to their neighbors and RSUs. In this case, every toll station has a Local Certification Authority (LCA), and nodes have to switch certifications when migrating from one zone to another. The LCA generates security credentials for vehicles. Additionally, it gathers information from observations of security violations in the nearby toll zone. A Central Trusted Authority (CTA), which is in charge of distributing digital certificates for the RSUs, preserving a Certificate Revocation List (CRL) containing the revoked certificates and analyzing the security reports sent by the LCAs, receives these observations and the security reports produced by the LCA. We assume the LCA and CTA to be robust and difficult to manipulate. We suppose that the CTA is strong in the sense that it has enough processing power and storage. In contrast to the LCA, the CTA should be able to identify the vehicle's authentic identification.

B. QoS MODEL

The QoS model that is introduced in this subsection considers the design differences that exist between IEEE 802.11 VANETs and 4G networks. Let v be a vehicle in a tree topology τ. We denote by α the route on the tree τ connecting to the gateway vehicle on that tree. The path is described as $\alpha = [v_1, v_2, \ldots, v_n]$ where v_n is the vehicle gateway of the tree, which is connected to an RSU through the 4G Network, v_1 is a leaf node vehicle and each vehicle $v_j (j \epsilon \{i, \ldots, n-1\}$ is an intermediate node attached to v_{j+1}. We denote by Q_v the QoS vector requested by vehicle v. It is expressed as a tuple: $Q_v = (D_v, L_v, T_v, R_v)$ of four metrics. The first QoS metric, D_v is a measure of the transport delay over route α. It is computed by a vehicle as follows:

$$D_{v_i} = \sum_{j \in [i, n-1]} d_{(v_j, v_{j+1})} + d_{(v_n, RSU)} \tag{1}$$

where a) $d_{(v_n,RSU)}$ represents the traffic residence delay in the buffer of the gateway vehicle v_n, in addition to the transmission delay between v_n and the RSU; and b) $d_{(v_j,v_{j+1})}$ denotes the delay between two consecutive nodes v_j and v_{j+1}. This delay is computed as the sum of the channel access delay, the decoding delay, and the transmission delay. Vehicle v_i calculates the average packet loss, denoted as L_{v_i}, which constitutes the second QoS metric. It is equal to:

$$L_{v_i} = max\{l_{(v_i,v_{i+1})}, \ldots, l_{(v_{n-1},v_n)}, l_{(v_n,RSU)}\} \tag{2}$$

where $l_{(v_j,v_{j+1})}$ is the packet loss of the link connecting vehicles v_j and v_{j+1}. A loss $l_{(v_j,,v_{j+1})}$, which, according to vehicle v_j, represents the proportion of frames that the decoder will discard in v_{j+1} if the packet arrival time is longer than the playback deadline. $l_{(v_n,RSU)}$ is the packet loss of the link connecting the RSU to the gateway vehicle v_n. Vehicle v calculates the available throughput T_v, which is the third quality of service (QoS) metric. The value of this parameter is determined by subtracting the bandwidth utilized by the gateway vehicle from the RSU via the 4G link, from the total bandwidth consumed by all vehicles in the tree. The quantity is expressed as:

$$T_v = T_{(v_n,RSU)} - \sum_{v \in \tau} (c_v + \rho_v) \tag{3}$$

$T(RSU, v_n)$ stands for the maximum throughput that the LTE link between the gateway vehicle v_n and the RSU can support. c_v stands for the flow peak rate associated with the traffic that vehicle v transmits, and rho_v stands for the average bandwidth of that traffic flow. The RSU estimates $T_{(RSU,v_n)}$ using the resource blocks already allocated by the RSU and the channel quality indicator (CQI) transmitted by the gateway vehicle v_n. The final QoS metric is the route lifetime, denoted as R_v, which is evaluated at vehicle v. It is expressed by:

$$R_{v_i} = min\{r_{(v_i,v_{i+1})}, \ldots, r_{(v_{n-1},v_n)}, r_{(v_n,RSU)}\} \tag{4}$$

where $r_{(v_j,v_{j+1})}$ denotes the link lifetime between vehicle v_j and vehicle v_{j+1}, while $r_{(v_n,RSU)}$ represents the link lifetime between gateway vehicle v_n and the RSU. We designate by the lifetime of a link (v_j, v_{j+1}) the amount of time that passes before v_j is no longer covered by v_{j+1}. It is equal to:

$$r_{(v_j,v_{j+1})} = (TR_{v_j} - d_{j,j+1})/|s_{v_{j+1}} - s_{v_j}| \tag{5}$$

where TR_{v_j} represents the vehicle v_j's transmission range, $d_{j,j+1}$ denotes the distance between v_j and v_{j+1}, and s_{v_j} designates the velocity of the vehicle v_j. The computation of $r_{(v_j,v_{j+1})}$ is simple in all other scenarios.

C. VEHICLE ATTACHMENT

A vehicle must carry out the following procedures in order to create a new connection or request a new service:

a: STEP 1

In order to establish its own quality of service (QoS) requirements, it generates a three-tuple set of information denoted as $QV^* = \langle D^*, L^*, T^* \rangle$, which specifies the maximum allowable delay, the maximum acceptable packet loss, and the requested throughput, respectively.

b: STEP 2

When a Roadside Unit (RSU) is available and the vehicle is within its coverage range, the vehicle periodically examines the Connection Advertisement messages (CAD) transmitted by neighboring vehicles and the RSU for a duration of time $\triangle t$.

c: STEP 3

From the CAD messages it receives, it derives the four-value QoS vectors. Then, in order to choose the node to which it will connect, it determines whether all the necessary QoS metrics are satisfied by some of these vectors.

d: STEP 4

The process involves generating an Attachment Request (AR) message, which will be sent to the selected node. This message contains the extracted information about the surrounding vehicle's identification and the path connecting it to the RSU. If no offer can match the vehicle's Quality of Service (QoS) criteria, it should either wait for new offers or modify its intended QoS.

e: STEP 5

The RSU decodes the received AR message to identify the newly connected vehicle and determine the required QoS. Upon computing the newly attainable data transfer rate, it produces a revised QoS vector and transmits an updated

CAD message (including the revised QoS vector) to the gateway vehicle. Additionally, it incorporates the new vehicle into the database.

f: STEP 6

After receiving the new CAD message acknowledging its request, the vehicle begins utilizing the requested service. A mobility management strategy is created in conjunction with the attachment algorithm to address the QoS requirements of a vehicle as it travels over the highway network. For this reason, two requirements—providing the necessary QoS and certificate validation—must be met with each handover as long as the cars move from one toll zone to another or from one tree to another.

Our system manages two different handover types: intra-zone handover and inter-zone handover. Our idea intends to: a) minimize the handover delay; b) minimize the frequency of handovers in order to avoid resource waste and QoS degradation; and c) minimize the likelihood that a handover will fail due to a lack of resources. In these circumstances, the vehicle starts a handover in two circumstances. Initially, when it detects a decline in the QoS parameters that were originally sought.

When the quality of the link between it and its parent, the route lifetime, the route delay, or the packet loss rate fall below the desired value, QoS degradation is in fact identified. Second, when the QoS demand for a new service cannot be met by the already available route. Thirdly, when a predetermined amount of time passes with no communication from its parent.

Consider vehicle B as a node that requires a handover to be established. It begins by listening to the broadcasted CADs and then extracts the routes from each CAD message that meet its QoS requirements. After that, it saves them in a route list, let's say θ. Second, it alerts its real parent vehicle, which must then deliver the route list to the RSU, in a message. From θ, the RSU chooses the top offers. An inter-zone handover is established if the new point of attachment is found in a neighboring zone. The procedure for revocation of certificates is used in this situation. Fig. 3 describes the attachment process.

In summary, VANET tree topology can be modified to maintain QoS metrics like throughput, jitter, and packet loss while modifying routing in dynamically changing speed scenarios. By prioritizing nodes for routing based on their proximity to important infrastructure locations or high-speed vehicles, we can maintain quality of service while guaranteeing prompt and effective message delivery.

Furthermore, nodes are arranged in a tree hierarchy to achieve application access optimization. Lower-level nodes can access these services through effective routing channels within the tree, whereas higher-level nodes may have direct access to critical applications. Dynamically repositioning nodes inside the tree can reduce latency and improve communication performance when they move quickly or fluctuate in speed. Although lower-level nodes can reach these services through effective routing pathways within the tree, higher-level nodes may have direct access to vital applications. However, the tree uses real-time traffic data, vehicle movements, and its hierarchical structure to determine the optimal routing paths for message transfer, thereby minimizing message transmission delays and packet losses.

Finally, to detect and mitigate potential difficulties like congestion, latency spikes, or packet losses, a QoS monitoring and control mechanism is integrated into the tree-based routing architecture.

IV. VEHICLE DIGITAL CERTIFICATE MANAGEMENT

The format used for a vehicle certificate partially adheres to the X.509 fundamental standard for a public key infrastructure (PKI). The issuing authority has granted a provisional identity known as the subject name or certificate holder. This is the first of two variances. Second, the certificate can have a few extra fields by using a field. Extensions for certificates offer a mechanism to add details such as different topic names, fundamental limits, usage limitations, policies, and vehicle patterns. It is possible to tell whether a certificate is a CA by looking at its Basic Constraints extension, which also indicates whether the subject of the certificate is permitted to issue child certificates. The alternative subject name is an optional parameter that allows the certificate issuer to include other names or information (such as an email address or a Universal Resource Identifier). The usage limits specify the key's function within the certificate as well as the authorized highway toll zone. The policy extension shields the issuer from liability and provides details on the CA policy that the certificate was issued under.

The vehicle pattern extension also includes an encrypted fingerprint created for the entering vehicle at the toll zone entrance and information about the tag used to issue the certificate. The car reads the information from the tag and records it on the certificate to aid in the vehicle's verification at other toll locations. The vehicle fingerprint can be created using a variety of methods. A camera can be used, in particular, to produce precise data on various vehicle attributes. Afterward, the data can be hashed and written to the certificate. The validating system can put a camera in and check the fingerprint using the content of the linked tag. The method utilized to create and duplicate the fingerprint will determine how robust the authentication is. It is easy to believe that this level is equivalent to or greater than the level offered by X509 v3. The steps for certificate development, delivery, renewal, and revocation are described here. We specifically demonstrate the role played by tags in the creation and validation of certificates.

A. CERTIFICATES DELIVERY/GENERATION

The LCAs installed on the perimeter of every toll zone generate certificates for each vehicle, expecting that each time the vehicle enters a new zone, it should acquire a

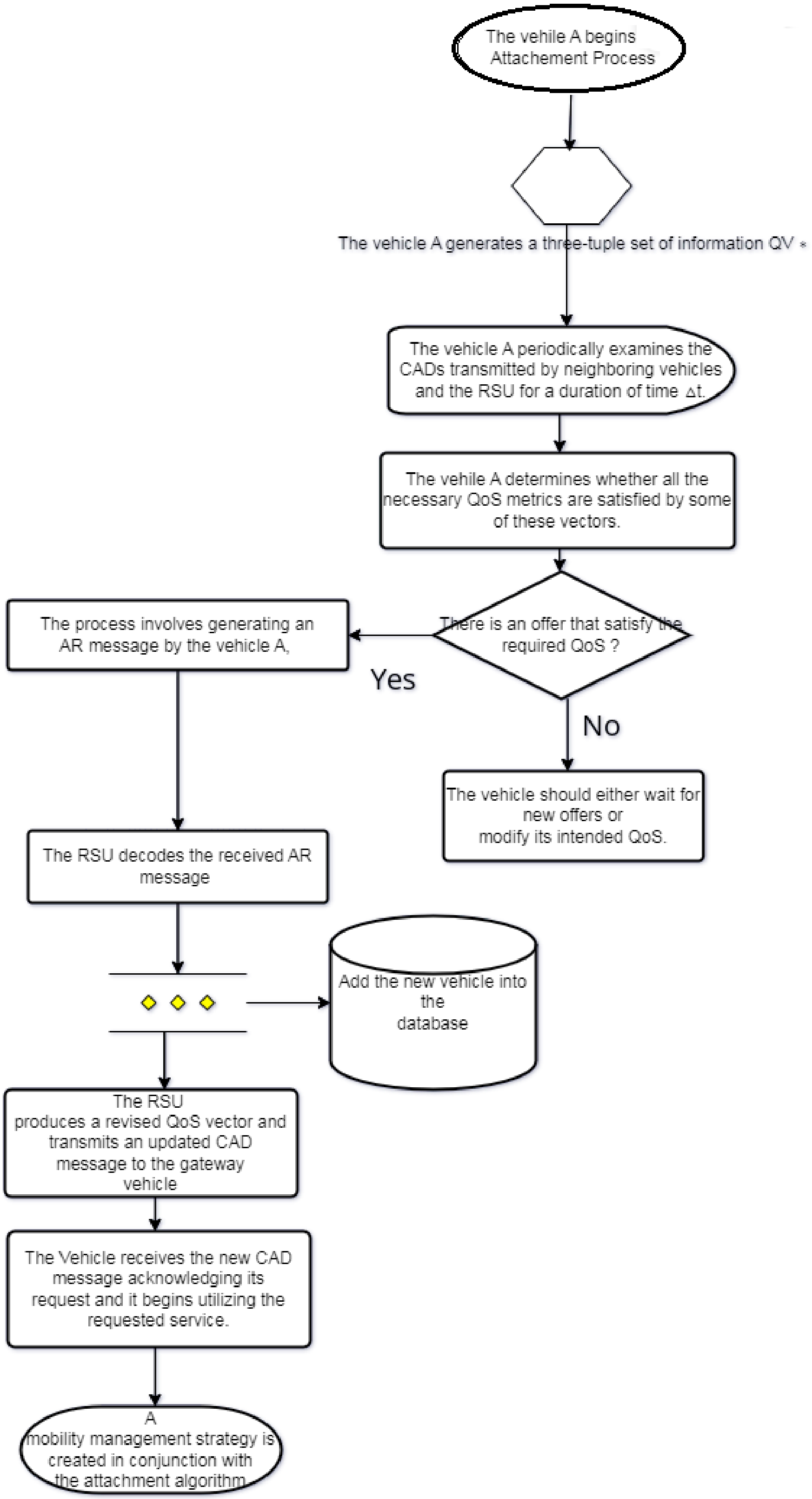
The vehile A begins Attachement Process
The vehicle A generates a three-tuple set of information QV *
The vehicle A periodically examines the CADs transmitted by neighboring vehicles and the RSU for a duration of time Δt.
The vehile A determines whether all the necessary QoS metrics are satisfied by some of these vectors.
There is an offer that satisfy the required QoS ?
Yes
The process involves generating an AR message by the vehicle A,
No
The vehicle should either wait for new offers or modify its intended QoS.
The RSU decodes the received AR message
Add the new vehicle into the database
The RSU produces a revised QoS vector and transmits an updated CAD message to the gateway vehicle
The Vehicle receives the new CAD message acknowledging its request and it begins utilizing the requested service.
A mobility management strategy is created in conjunction with the attachment algorithm

FIGURE 3. Attachment process.

legitimate certificate for that zone. There are various stages involved in the certificate generation process.

a: STEP 1 (INITIAL CERTIFICATE REQUEST)

The vehicle enters the tagged surface and passes over certain RFID tags (on the road lane it is using) when it reaches the first toll zone entrance point. The vehicle's RFID reader activated the tag and retrieved the positional data noted in letter A. The 4-tuple $A = (n_1, \ldots, n_4)$ represents the position information, where n_1 is the lane number, n_2 is the direction of travel, n_3 is the distance to a reference point on that lane, and n_4 is a random number that the system generates each time the RFID tag is read. If a vehicle is going from one zone to another, the request includes the vehicle's identify, tag information, and certificate information.

b: STEP 2 (VEHICLE REGISTRATION)

The toll system (or certification authority) uses a recognition algorithm based on photo processing and RFID technologies to confirm the identity of the vehicle. In actuality, beacons made of active RFID tags embedded in the road surface are utilized to precisely track a vehicle's location inside a toll booth at all times. In actuality, the active tags securely notify the toll system of a vehicle's location whenever one passes through the marked area. To confirm that the vehicle exists and that its location is accurate, the message that was delivered includes the recorded position information. The car request arrives at the same moment.

c: STEP 3 (CERTIFICATE ISSUANCE AND DELIVERY)

A pair of private and public keys must be generated by the vehicle, and the public key must be sent securely (using the certification) to the toll system. The certificate is issued and provided to the vehicle, following confirmation of the connection between the delivered public key and the private key. The newly created certificate is distinguished by a brief validity period, which is selected in consideration of the vehicle's average speed and the separation between the toll station and the upstream toll point that will follow. Furthermore, the CTA receives all the used data, including tag content and images, so it may update its LDAP, verify the integrity of some data, and determine the original identification of the vehicle. With two exceptions, the development and distribution of a digital certificate for a vehicle transitioning from one zone to another happens in the same way. First, the request for the creation of a new certificate sent in the first step needs to be confirmed by the new toll system (during the second step) using the old certificate. If the old certificate is still valid, the new toll system should revoke it (on the fourth step) before presenting the new certificate. However, if the vehicle is still in the middle of the zone and not close to a toll point when the vehicle certificate finishes its lifetime and becomes invalid, the renewal of the certificate may still be used. In this situation, two options are available:

1) Until it reaches the toll station, the vehicle cannot utilize the certificate.
2) As long as the vehicle certificate's extension profile permits it and the CTA has been notified by the service provider, the vehicle may continue to access a service it had before its lifetime expired.

There are three various types of certificate renewals: renewal upon leaving a toll zone, renewal when entering a new zone, and renewal at the expiration of the certificate's lifetime. The first happens while the car is leaving the highway system. The second type relates to the scenario where the vehicle changes zones. The third situation occurs when a vehicle stays in the same zone for an extended period of time after its certificate expires.

B. CERTIFICATE REVOCATION

Typically, the revocation procedure is required to ensure exclusivity (at any time) of the certificates active within a toll system. The attached process must be accurate and reliable, and the certificate's information must be kept up-to-date as well. In particular, when a vehicle receives new certificates as it enters a new zone while the certificate it received in the most recent zone is still valid (as it has neither expired nor been revoked), the vehicle acquires two valid certificates: one is delivered in the most recent zone, and the other is a new certificate that is automatically delivered without checking the last-generated certificate's expiration time, if the old certificate has not been revoked. Given that it owns two certificates created with distinct identities, the owner of the two certificates in that situation, may launch a number of attacks (such as the Sybil attack).

To prevent such malicious conduct, the system must first verify that the old certificate is still valid and revoke it if necessary. After verification, the authorized authority can start creating the new certificate. The LCAs and the TCA are the only entities capable of revocation. This latter entity is responsible for managing and disseminating a certificate revocation list (CRL) that lists all serial numbers for certificates that have been revoked; as a result, entities possessing those (revoked) certificates should no longer be trusted. When relying on a certificate, best practices dictate that the status of the certificate be verified. The Online Certificate Status system (OCSP), a certificate validation system that requires less network bandwidth and permits near real-time status checks for high volume or high value applications, is an alternative to using CRLs.

Since the LCAs and TCA are the only entities responsible for certificate revocation and that the LCAs can be assumed to be attached to a reliable and continuously connected network, an OCSP can be built to allow access in a real-time manner to the certificate status so that the revocation list at the TCA is updated every time a new certificate is generated. Therefore, using the tree-based architecture, one can assume that a vehicle is able to access the CRL list if the RSUs are kept aware of the revoked certificates. For this, our approach builds a protocol that allows CTA to periodically report to the RSUs the newly revoked certificate in the zone where they are located. Therefore, the only entities that may not be aware of the newly revoked certificates are those that are not attached to a tree. These nodes cannot access any service. It appears clearly that the storage of such information is reduced since the number of vehicles in a toll zone for any period of time is limited.

Let us now discuss how and when a LCA revokes a certificate. When a vehicle enters a zone where a toll point is available, the LCA attached to that point becomes aware of the vehicle's arrival since the RFID tags on the road lane taken by the vehicle for which it does not have a valid certificate. The LCA is activated to proceed for the identification of vehicles. If the vehicle holds a digital certificate, the LCA will check the validity of the certificate and decide whether it needs to be revoked. If it decides to generate a new certificate, it first revokes the old certificate, if it is still valid. For this, it uses the OCSP protocol to inform the TCA.

Therefore, the certificate's lifetime is a major factor in providing almost real-time revocation updates and checks. It is also important for reducing the revocation overhead. It can be estimated using the average speed of vehicles in a zone as well as the highway map (the distance between toll stations and the uncovered inter-zone). LCAs share the data history collected from RSUs regarding vehicle movement and zone residency time (i.e., entry and exit time to and from RSU coverage) to set up this period of time.

V. VEHICLE AUTHENTICATION IN SECURE VANET

In order to safeguard driver and passenger privacy and thwart security breaches that specifically target VANET components, we suggest an authentication scheme in the following section that utilizes RFID systems and an ad hoc public key infrastructure. For this, we assume that every vehicle has a globally verifiable identity by the TCA using the details included in the vehicle's request for a certificate and/or the vehicle's license plate number. To enable authentication and avoid attacks on vehicle privacy, we assume that when a vehicle is added to the home network for the first time, a temporary identity (T_i) is assigned in addition to the global identity. The identity (T_i) is saved in the CTA and the vehicle so that it can be utilized while in the same zone.

A. THE AUTHENTICATION PROCESSES

Two types of authentication are performed in our system, namely, the authentication at registration, authentication at zone boundary crossing, and authentication based on certificate presentation. Authentication at registration is performed on the arrival to a toll point of a vehicle not holding a certificate. In that case, a picture of the vehicle is taken after determining its position on the road line. Then, the content of the request for a certificate is sent to the TCA for verification of the license plate number and the coherence of the data included in the request, the vehicle tag, and the useful patterns in the picture with respect to the data available in the TCA database. If the verification is positive, the collected data is hashed with the picture content, a temporary identify is generated, and a certificate containing the hash value, the collected data, and the new identity is generated by the LCA. The certificate is finally delivered to the vehicle and sent to the TCA.

The authentication at zone boundary crossings is performed by an LCA on arrival to a toll point. It operates in three steps, as follows:

a: STEP 1

Active RFID tags are positioned in the road lane alongside the vehicle and function as beacons to precisely ascertain the location of the vehicle in the toll station at the time of its stop.

b: STEP2

The vehicle certificate is presented to the LCA. If the time field of the certificate is valid and the certificate was not revoked, a picture of the vehicle is generated based on the information written on the certificate (information related to the position of the vehicle when the first picture has been taken). If the time field content is not valid, a certificate renewal is triggered.

c: STEP 3

The picture content is hashed and compared to the picture hash value in the certificate. If the matching is valid, authentication is demonstrated, and the TCA is informed about the new position of the vehicle. If the hash values do not match the new picture and the certificate are sent to the TCA, where the images are analyzed and the useful vehicle features are matched. If the pictures deliver the same feature, then the vehicle is authenticated. We notice in the case that after authenticating the certificate on the zone boundary, the certificate is revoked and a new certificate is generated (with a new temporary identity), if the vehicle is entering a new zone. Furthermore, the captured image is used not only to extract information for the vehicle physical authentication in the toll station that generated the certificate, but it is also used by the following LCA to verify that the vehicle requesting a new certificate is the true owner of that valid certificate. In fact, the old image is embedded in a Notification Message (NM) sent to the TCA. This image will be utilized to do a verification based on a comparison of the extracted information from the old image and the newly captured image. The car is authenticated if the comparison demonstrates that it is the same vehicle.

Any node on the VANET can request vehicle authentication based on certificate presentation. The RSU does this by simply doing certificate validation and determining if the certificate has not been revoked based on the delta CRLs that the RSU receives on a continuously.

The proposed vehicle authentication procedure can be triggered by the VANET whenever one of the following events occurs: a) the vehicle enters the network and requests a connection for the first time; b) the vehicle requests a change

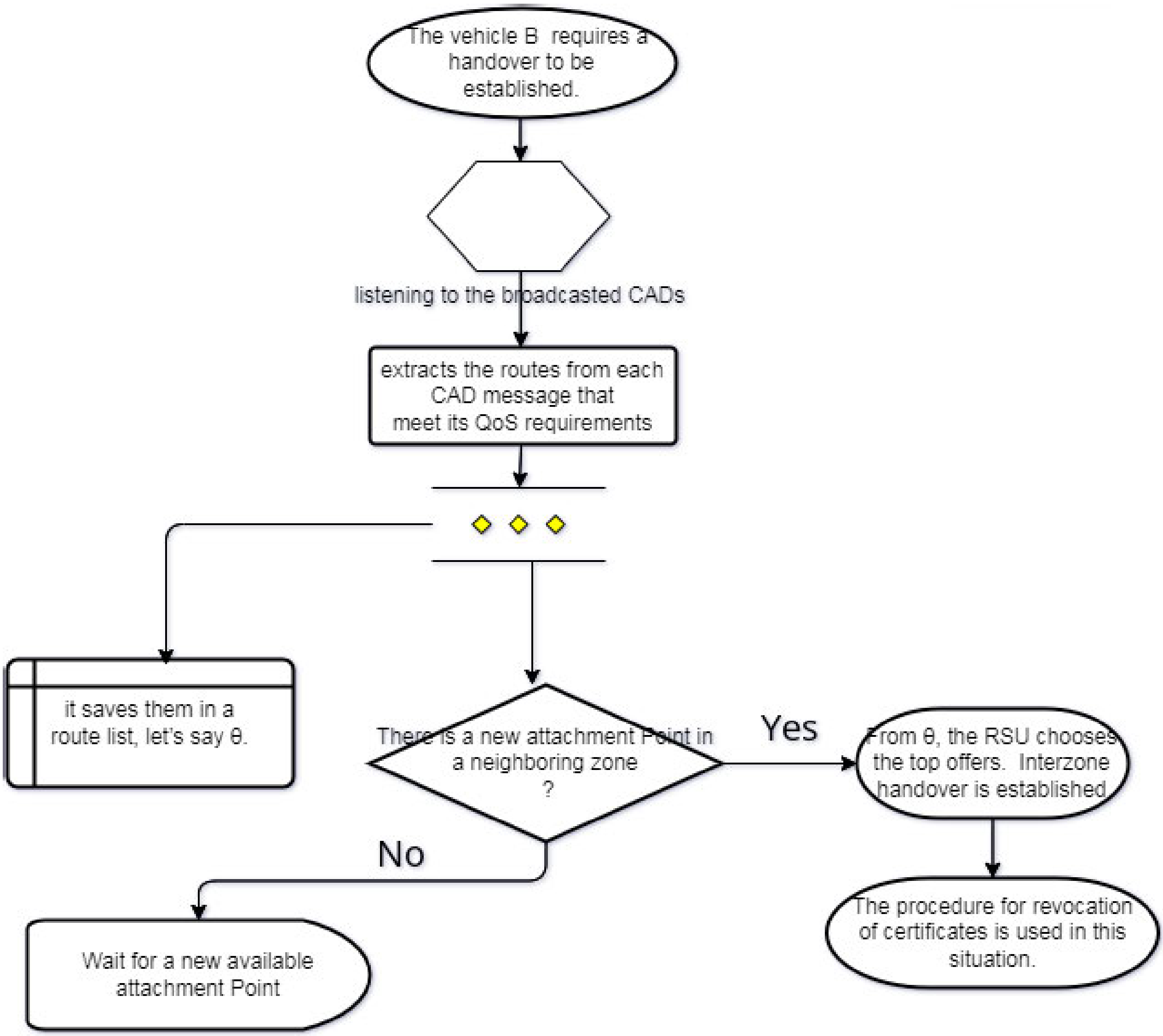
The vehicle B requires a handover to be established.
listening to the broadcasted CADs
extracts the routes from each CAD message that meet its QoS requirements
it saves them in a route list, let's say θ.
There is a new attachment Point in a neighboring zone ?
Yes
From θ, the RSU chooses the top offers. Interzone handover is established
No
Wait for a new available attachment Point
The procedure for revocation of certificates is used in this situation.

FIGURE 4. Moving management.

of attachment point due to node mobility (i.e., handover); or c) the vehicle remains connected but its updated location information announces that it has reached the next toll station. Fig. 5 describes the authentication process.

B. CERTIFICATE VALIDATION

In this subsection, we describe the validation process that is appropriate for validating the special digital certificate defined in the previous sections. This validation process is built through four checks: the certificate lifetime, the local authority signature, the ownership, and the vehicle identity.

a: CERTIFICATE LIFETIME CHECK

The generated certificates are only valid for a short period of time allowing the vehicles to circulate in the toll zone with a valid certificate until they get out of the zone. For this, the LCA includes an expiration time when it signs a certificate assuming that all LCAs and RSUs are timely synchronized. One receiving a vehicle certificate, the LCA checks whether its local time ranges within the time interval defined on the certificate. To reduce the number of revocations, the LCA should set a lifetime that strikes a balance between: a) selecting a long lifetime period, which avoids renewing the certificate frequently but may indicate the need to revoke the certificate if the mobile exists and remains in the same zone while its certificate is still valid; and b) selecting a short lifetime period, which avoids revoking the certificate but causes the mobile to generate multiple renewal requests for the same certificate.

b: SIGNATURE VALIDATION

As previously stated, the proposed secure VANET has a hierarchical system architecture comprised of a central trustworthy authority (CTA) and local certificate

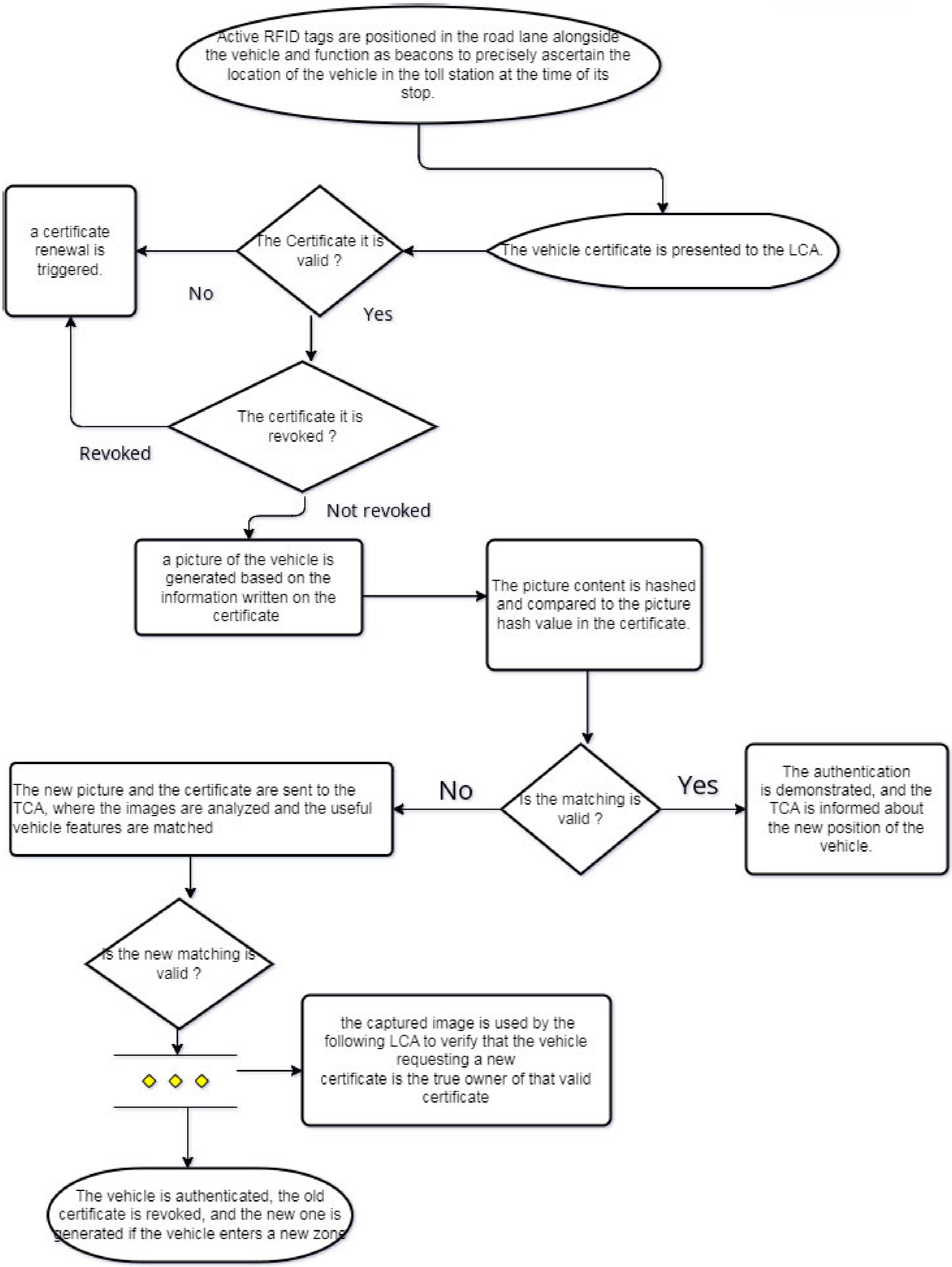
Active RFID tags are positioned in the road lane alongside the vehicle and function as beacons to precisely ascertain the location of the vehicle in the toll station at the time of its stop.
The vehicle certificate is presented to the LCA.
The Certificate it is valid ?
No
Yes
a certificate renewal is triggered.
The certificate it is revoked ?
Revoked
Not revoked
a picture of the vehicle is generated based on the information written on the certificate
The picture content is hashed and compared to the picture hash value in the certificate.
Is the matching is valid ?
No
Yes
The authentication is demonstrated, and the TCA is informed about the new position of the vehicle.
The new picture and the certificate are sent to the TCA, where the images are analyzed and the useful vehicle features are matched
Is the new matching is valid ?
the captured image is used by the following LCA to verify that the vehicle requesting a new certificate is the true owner of that valid certificate
The vehicle is authenticated, the old certificate is revoked, and the new one is generated if the vehicle enters a new zone

FIGURE 5. Authentication process.

authorities (CAs) spread throughout the network. When digital certificates are utilized, the nodes must have LCAs public keys in order to validate the signature. To accomplish this, the vehicle can use the root certificate included in it to validate the signature of the authenticated entity.

c: OWNERSHIP CHECK

The ownership validation allows for verifying the reliability of the temporary identity presented in the certificate. After validating the public key, authentication of the vehicle is involved by validating its private key. The private key is validated to avoid malicious vehicles using the identity of a valid one to transmit faulty information. In order to ensure this validation, the vehicle is asked to sign a message using its private key. Once the received message is properly decrypted by the local authority using the corresponding public key, this provides high level of reliability.

d: VEHICLE IDENTITY CHECK

To prevent malicious vehicles from using a valid certificate, the vehicle owner of the certificate is validated by comparing pictures taken at the toll station. As it is explained in Section IV, taken pictures will be exchanged between neighboring LCAs using the notification message, NM, in order to achieve the vehicle's physical authentication. To achieve this objective, we propose to follow the following steps:

1) Interest point detector, e.g. license plate or rear view mirror. Note that we can use an image processing algorithm defined in the literature to extract the key points from the vehicle photo,
2) Represent the images with a set of local features based on the Local feature descriptor;
3) Compare the local features across the images and find the common local features.
    a) If the comparison of vehicle photos based on the computation made gives a positive result and justifies that it is the same vehicle owner of the certificate, the vehicle validation process is achieved successfully.
    b) Otherwise, a malicious vehicle is detected and the certificate is revoked.

C. SECURITY FEATURES

Our secured network equips a wide variety of safety features to safeguard against various threats and ensure the confidentiality, integrity, and authentication of vehicle communications. These features include resistance against Sybil attacks, denial of service protection, certificate management, temporary identity uniqueness, replay attack prevention, and vehicle privacy safeguards.

1) DENIAL OF SERVICE PROTECTION

A denial-of-service attack cannot be undertaken against an LCA. In fact, the vehicle's RFID scanners only establish a connection with the LCA when they identify the location information from road tags on the lane they are following. The request encrypts the vehicle data as well as the position information using the toll station's public key and delivers the encrypted content to the toll system. Any malicious user attempting to impersonate a legitimate vehicle will not be able to obtain an answer from the toll system because the toll station decrypts the vehicle request and checks whether the position information in that request message was recently read from the road tags when the vehicle entered the tagged surface.

2) CERTIFICATE MANAGEMENT

In our proposed system, the use of unique, valid certificates for every vehicle in a toll zone adds another layer of security. Generating certificates upon entry to a zone and revoking previous certificates ensure that each vehicle has an up-to-date and valid credential for communication within that specific zone. This approach minimizes the risk of unauthorized access or misuse of certificates. Additionally, the mechanism to invalidate certificates if a vehicle spends more time than expected in a zone helps maintain the security and integrity of the certificate management system, further enhancing the overall security posture of the proposed system deployment.

3) RESISTANCE AGAINST SYBIL ATTACKS

No Sybil attack can be performed on the toll system. In a Sybil attack, a malicious user can pretend to use many fake or Sybil identities. A defense against Sybil attacks enables a verifier node (e.g., a LCA, a vehicle) to decide whether to accept another node's identity. In our secure VANET a Sybil attack is prevented because the temporary identities occurring in the certificates are given by the LCAs and the only way to claim an identity is to submit a certificate containing that identity. In the above validation process, the ownership check will certainly detect a faulty certificate.

4) TEMPORARY IDENTITY UNIQUENESS

The temporary identities are unique. Indeed, we can generate the temporary identity by concatenating the LCA identity with a random value. Because the LCA identities are different, the hash function will ensure that the generated hash values are distinctive.

5) REPLAY ATTACK PREVENTION

There is no way to initiate a replay attack. Even if a malicious vehicle attempts a replay attack and regenerates the certificate request, the system will identify this activity. In fact, because the random number contained in the RFID tag and the detected node location do not match, the second phase is skipped and no certificate is created.

6) PRIVACY PROTECTIONS FOR VEHICLES

To some extent, vehicle privacy is preserved. In reality, to protect the car's privacy and prevent neighbors from tracing it from one zone to another, each vehicle employs a temporary identity that is valid for the duration of the contained certificate. Furthermore, to avoid the possibility of

TABLE 2. Further attacks, their threats and countermeasures.

Attacks	Threats	Countermeasures
Side-Channel Attacks	Side-channel attacks exploit information leaked during the normal operation of cryptographic systems, such as timing information, power consumption, electromagnetic emissions, or acoustic signals	Implement constant-time algorithms, use power analysis countermeasures, and employ shielding techniques to prevent information leakage
Physical Attacks on RFID Tags	Physical attacks on RFID tags include tampering, cloning, and jamming. Attackers could physically alter or duplicate RFID tags or disrupt their communication	Use tamper-resistant RFID tags, implement tag authentication protocols, and deploy signal obfuscation techniques to protect against physical tampering and cloning
Advanced Persistent Threats (APT)	APTs involve long-term, targeted attacks aimed at compromising specific vehicles or infrastructure components	Use continuous monitoring, threat intelligence, and incident response planning to detect and respond to APTs. Ensure regular software updates, conduct security audits, and follow robust software development practices to minimize vulnerabilities
Software Vulnerabilities	Software vulnerabilities can be exploited to gain unauthorized access or control over VANET components	Ensure regular software updates, conduct security audits, and follow robust software development practices to minimize vulnerabilities
Insider Threats	Authorized individuals might misuse their access to compromise the system, either maliciously or accidentally	Implement strict access control policies, monitor user behavior, and follow the principle of least privilege to reduce the risk of insider threats
Privacy Attacks	Attacks that aim to track or disclose the private information of drivers and vehicles	Use pseudonymization, temporary identities, and strong data encryption to protect privacy
Eavesdropping	Unauthorized interception of communication between vehicles and infrastructure	Encrypt all communications to ensure confidentiality and prevent eavesdropping

another vehicle utilizing the valid certificate, the certificate owner must be confirmed by a photo taken at the toll station. Thus, a recognition function is proposed based on the taken photo, and only a trustworthy LCA may determine the relationship between the certificate and the taken photo.

D. FUTURE SECURITY ANALYSIS

Our presented security analysis focuses specifically on Sybil attacks and replay attacks due to their high relevance and frequency in the context of vehicular ad hoc networks (VANETs). These attacks were selected based on their critical impact on VANET security and their ability to undermine the quality of service (QoS) parameters that our proposed authentication scheme aims to improve. Although side-channel attacks, physical attacks against RFID tags, advanced persistent threats, and zero-day vulnerabilities are recognized as major cybersecurity concerns, our research was intentionally limited to threats that have a more direct impact in the VANET environment.

We plan to expand our analysis to include side-channel attacks and physical attacks on RFID tags, explore the implications of advanced persistent threats and zero-day vulnerabilities in the context of VANETs, and develop and integrate mitigation strategies for these additional threats into our proposed authentication scheme. The table 2 lists some attacks, their threats and countermeasures, In order to cover a wider range of potential threats.

VI. SIMULATION

The simulation makes it possible to fully comprehend how changing parameters affect the dynamics of VANETs. Thus, our goal is to understand how resource unavailability affects network performance, as well as how to provide a high quality of service (QoS) in terms of throughput. In addition, our objective is to assess some features of our VANET system, namely the best certificate lifetime considering vehicle speed and quality of service metrics (such as average delay and average blockage rate per vehicle).

A. SIMULATION MODEL

The simulation model involves specific scenarios for certificate management in VANETs:

1) **Certificate Generation**
   - Vehicles request a new certificate in two scenarios: when they enter the highway for the first time and when they change direction at a highway interchange.
   - This approach ensures that vehicles have valid certificates when they join the highway network or when they make significant changes in their route.

TABLE 3. Simulation parameters.

Roadway Map		
Covered Area	Number of exchangers	Number of lanes in each direction
30 x 64 km2	2 exchangers : three-way street for incoming and departing cars	3 lanes
Vehicles speeds		
Speed of vehicles in lanes 1	Speed of vehicles in lanes 2	Speed of vehicles in lanes 3
60km	80km	100km
Vehicle Communication Range	RSU communication Range	Simulation Period
200 meters	5000 meters	8000 s with a timeslot of 4 s

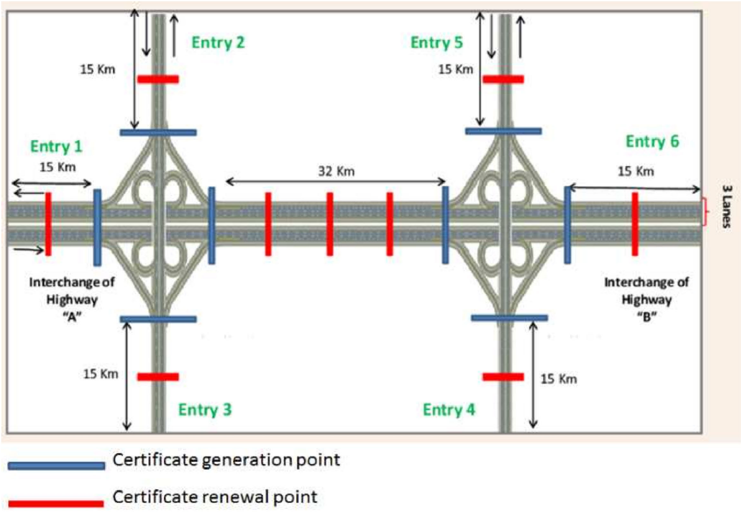
Entry 2
Entry 5
15 Km
15 Km
Entry 1
15 Km
32 Km
Entry 6
15 Km
3 Lanes
Interchange of Highway "A"
Interchange of Highway "B"
15 Km
15 Km
Entry 3
Entry 4
Certificate generation point
Certificate renewal point

FIGURE 6. Topology of the simulated network.

2) **Certificate Renewal**

- If a vehicle reaches a certificate renewal point while its certificate's lifetime has expired, the system presumes that the certificate is renewed.
- This mechanism helps maintain the validity of certificates and ensures that vehicles can continue operating securely within the VANET environment.

3) **Certificate Revocation**

- When a vehicle changes its heading at a highway interchange while its old certificate is still valid, the system revokes the old certificate.
- Revoking certificates in such scenarios helps manage security effectively, especially when vehicles change their routes or directions within the network.

The table 3 resumes simulation parameters: In our simulation model depicted in Fig. 6, we have additional conditions and procedures related to certificate management in VANETs.

1) **Certificate Management for Moving Vehicles:**· Vehicles can have their certificates generated, renewed, or revoked while moving within the network of roads. This dynamic certificate management ensures that vehicles maintain valid credentials as they navigate through the VANET environment.

2) **Certificate Management for Moving Vehicles:**· Certificates with expired lifetimes are renewed at renewal points, ensuring continuous validity. When a vehicle changes direction, the system verifies the old certificate's validity. If valid, the old certificate is revoked before issuing a new one. If the old certificate is invalid, a new certificate is directly issued without revocation. When a vehicle moves straight, a new certificate is generated only if the old one has expired at a generation point, preventing unnecessary certificate issuance.

Because the proposed system's defense against attacks is dependent on the usage of certificates, the goal of the first numerical experiment in the simulation is to investigate the variation in the average number of certificates per vehicle based on certificate lifetime and vehicle speed.

B. EXPERIMENTATION RESULTS

In the first and second simulations, we approximated the average number of Certificate Renewals (CRs) and Certificate Revocations (CVs) per vehicle based on the Certificate Lifetime and the speed of the vehicles. We adjusted the certificate lifetime from 200 to 1500 seconds in these simulations, performed the simulation for three pairs of

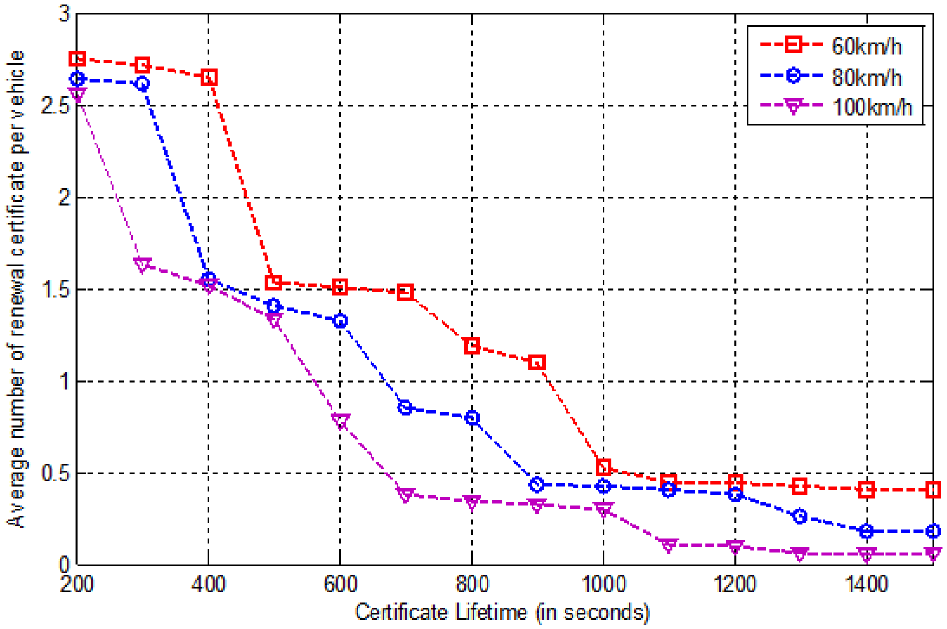

FIGURE 7. Average number of CRs per vehicle w.r.t. Certificate lifetime.

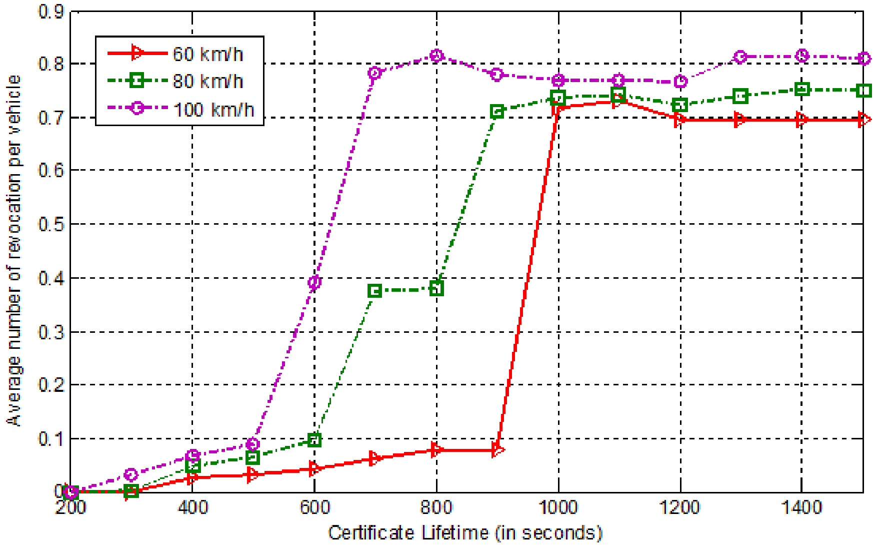

FIGURE 8. Average number of CVs per vehicle w.r.t. Certificate lifetime.

highway speeds of 60 km/h, 80 km/h, and 100 km/h, and fixed the vehicle arrival rate to 0.6. As shown in Fig. 7, the average number of renewed certificates falls when vehicle speed on the three-way roadway increases. Indeed, as vehicle speed increases, certificate lifetime grows, and the position of renewal locations remains constant, vehicles will rapidly approach the certificate renewal point, increasing the likelihood of possessing a valid certificate. Since long-term certificates take longer to renew during travel, the average number of certificate renewals drops as vehicle speed increases.

The average number of CVs increases when the speed of vehicles on the three-way roadway increases, as shown in Fig. 8. In fact, when vehicle speeds increase and certificate lifetimes increase, the likelihood of possessing a valid certificate when the vehicle changes direction at the highway exchanger increases. As a result, the average number of CVs per vehicle will grow if the certificate lifespan in the third simulation represents the average number of CRs per vehicle with respect to the certificate lifetime and the likelihood of staying in the same direction at the highway exchanger, indicated P. According to the 3D

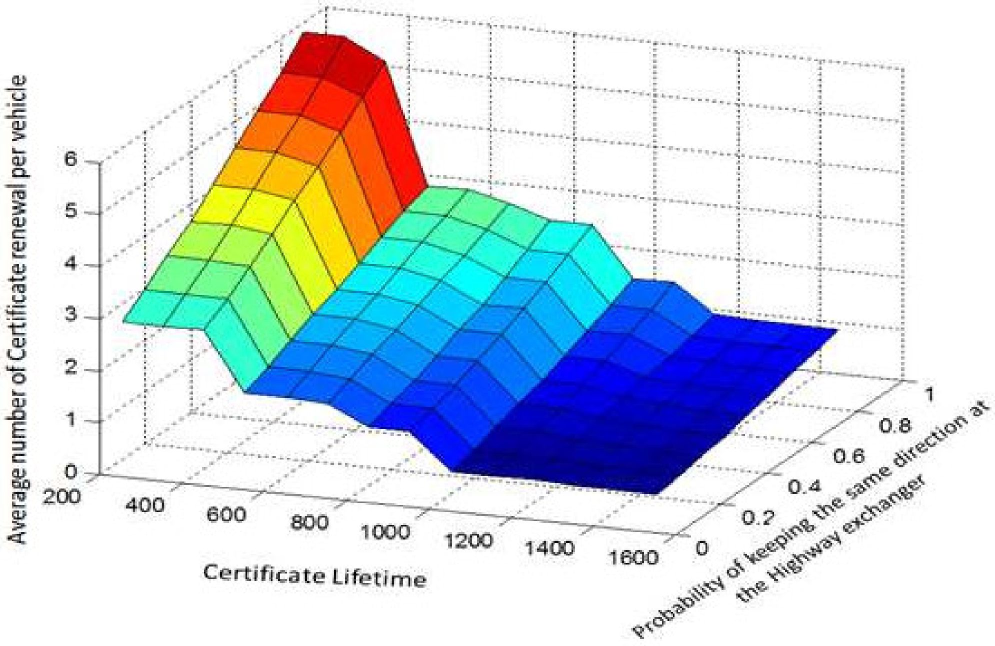

FIGURE 9. Average number of CRs per vehicle w.r.t to the probability of keeping the direction and certificate lifetime.

graph in Fig.9, the average number of CRs reduces as the certificate lifetime grows. Because the certificate's lifetime is long, it takes longer to renew the certificate during travel. Furthermore, the graph illustrates that when the probability, P1, increases, the average number of certificate renewals decreases at a decreasing pace, particularly for large values of the probability. However, when the certificate duration reduces, this decrease is particularly significant for high probability (P). In reality, as long as the probability P becomes significant, the vehicle must renew its certificate while maintaining the same orientation at the exchanger. In contrast to the limited certificate duration, the necessity to renew the certificate diminishes with a high probability. As a result, when the certificate duration is short, the average number of certificate renewals grows more significantly with high probabilities.

In the fourth simulation, we assess the average number of CRs per vehicle in relation to the certificate lifetime as well as the probability of changing direction at the highway exchanger, indicated P_2. The 3D graph, as shown in Fig.10, shows a rise in the average number of certificate revocations per vehicle as the certificate lifetime and the probability of changing the direction at the highway exchanger grow. Indeed, as the certificate lifetime increases, the likelihood of possessing a valid certificate when the vehicle changes direction at the highway exchanger increases, justifying the requirement for certificate revocation. Furthermore, as the probability of changing the direction of the exchanger grows, so will the number of certificate revocations. As a result, for lengthy certificate lifetimes and a high probability, P_2, the average number of certificate revocations is more important.

The sixth simulation assessed the vehicle's average latency during its connection. In this simulation, we suppose that revocation of a certificate takes 0.7 seconds. We also assume that a certificate renewal takes 0.2 seconds and that generating a certificate takes 0.4 seconds. As illustrated in Fig. 11, if the certificate lifetime does not exceed 1000 seconds, the longer the validity term of certificates, the shorter the average delay. In reality, as a certificate's lifetime increases, so does the possibility that vehicles will reach a renewal point with a valid certificate. Furthermore, the possibility of vehicles rescinding their certifications upon entering a zone is negligible. As a result, the average delay will reduce. In the other instance, as long as the certificate lifetime exceeds 1000 seconds, the average delay increases. In fact, if a vehicle uses long lifetime certificates, the certificate will be revoked at each revocation point, which will cost more than the renewal process. According to the simulation results, the shortest delay occurs when the certificate lifetime is equal to 1000 seconds.

In the simulation, whose results are presented in Fig. 12, we evaluate the average number of blockage per vehicle with respect to the vehicle arrival rate and the certificate lifetime. Noted that the blockage is detected when the vehicle doesn't find an attachment. point to be connected for the first time or when a handover process fails due to resource unavailability. Based on these results, we denote that if the lifetime of a certificate does not exceed 600 seconds, the average number of blockage per vehicle decreases when the certificate lifetime increases. In fact, as the lifetime of a certificate increases the probability that vehicles reached a renewal point with a valid certificate will decrease. Therefore, the certificate

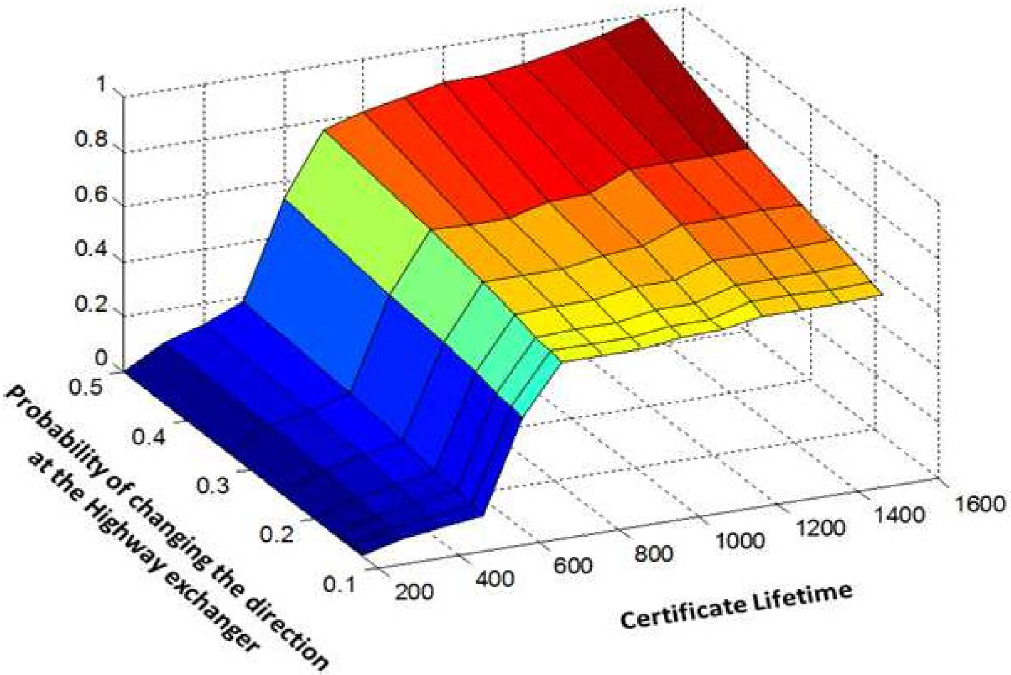

FIGURE 10. Average number of CVs per vehicle w.r.t Certificate lifetime and the Probability of changing direction.

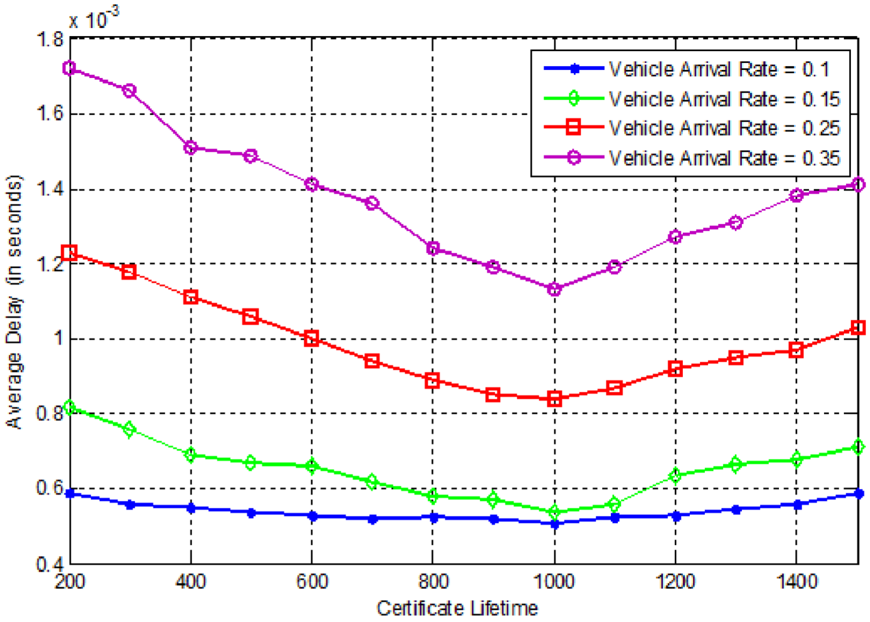

FIGURE 11. Average Delay w.r.t Certificate Lifetime.

renewal is the most important cause of the blocking when the certificate lifetime is less than 600. In the opposite case, as long as the certificate's lifetime exceeds 600 seconds the ratio of revoked certificates becomes greater than the ratio of renewed certificates. Thus, the average number of blockage increases when the lifetime of a certificate increases. In fact, using long lifetime certificates, a vehicle would reach a revocation point while the certificate is still valid. In this case, the certificate revocation is the most important cause of the blocking state.

In the next simulation, we estimated the average number of blockage according to the number of vehicles and the certificate lifetime for each lane of the highway, where; a) the average vehicle speed in lane 1 is 60km/h, b) the average vehicle speed in lane 2 is 80km/h, and c) the average vehicle speed in lane 3 is 100km/h. The results of this simulation are

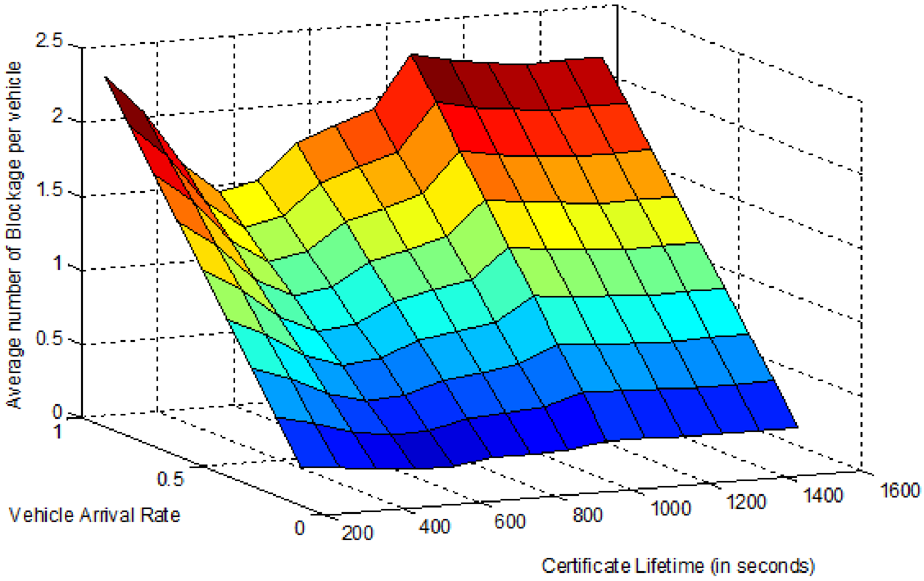

FIGURE 12. Average Blocking per vehicle w.r.t Vehicle Arrival Rate and Certificate Lifetime.

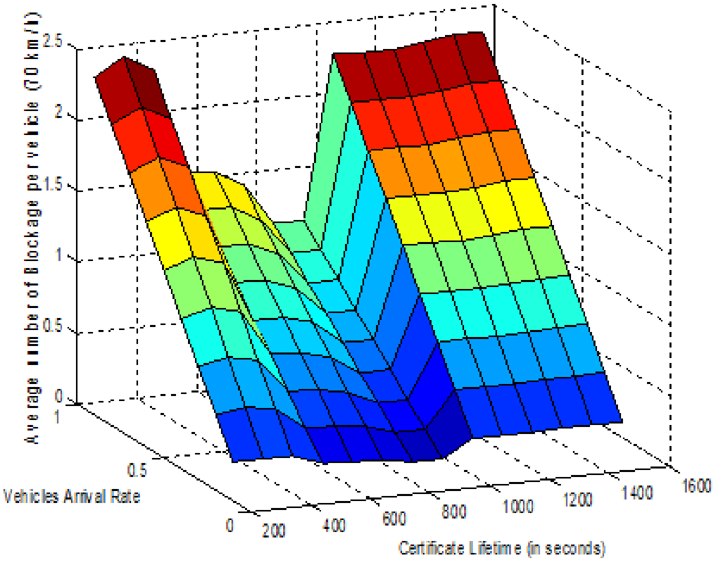

FIGURE 13. Average blocking per vehicle w.r.t vehicle arrival rate and certificate lifetime for lane 1.

depicted by Fig. 13, 14, and 15. We noted that the minimum blocking is shown when the certificate lifetime is equal to 800, 600, and 400 seconds when the average vehicle speed is equal to 70km/h, 80km/h, and 100km/h, respectively.

The last numerical experiment evaluates the blocking rate with respect to the vehicle arrival rate for two scenarios where the security solution is implemented or not. We assume that at each time slot (set to 4 sec) a vehicle can request an additional multimedia service with a probability equal to 10%. Each one of these services requires a bandwidth of T and has a duration equal to 200 seconds. The requested bandwidth T varies between a nominal value denoted T^{min} (set equal to 5Mbps) and $T^{min}+\triangle$, where $\triangle$ takes two values: 1 Mbps and 5 Mbps. Moreover, in this simulation, we also assume that the certificate lifetime is equal to 1000 seconds. Fig. 16 shows that both in a secured network or non-secured network, the blocking rate increases with the increase of $\triangle$. Indeed, as long as the required bandwidth T increases when $\triangle$ increases, the blocking rate increases due to the increase in the number of failed handovers because of the unavailability of free bandwidth. In addition, we notice that the blocking rate decreases while the vehicle arrival rate increases. In fact, as long as the network becomes dense when the vehicle arrival rate increases, vehicles are likely to find neighbor

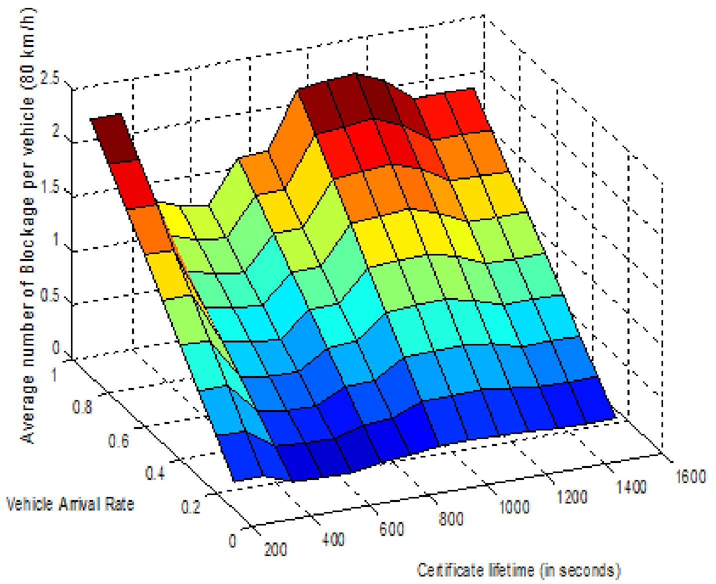

FIGURE 14. Average blocking per vehicle w.r.t vehicle arrival rate and certificate lifetime for lane 2.

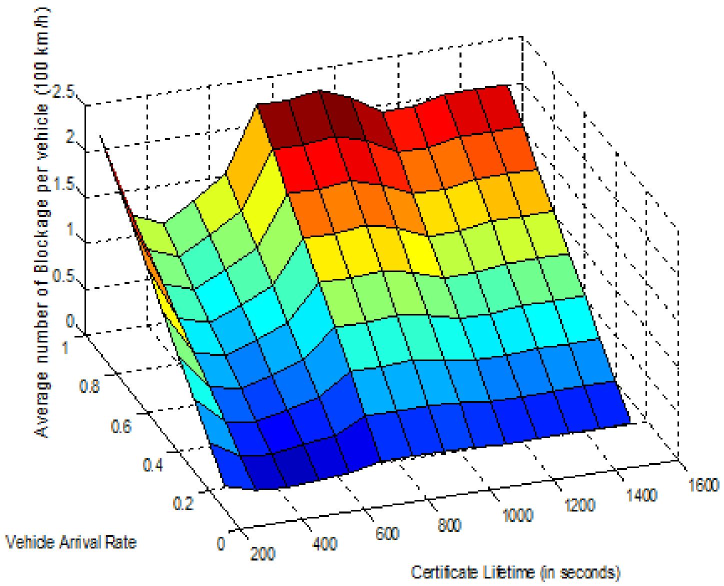

FIGURE 15. Average blocking per vehicle w.r.t vehicle arrival rate and certificate lifetime for lane 3.

attachment points (i.e., other connected vehicles) that meet their requirements, decreasing the blocking rate. Besides, based in these results, we demonstrate that the cost in terms of blocking of the proposed security strategies does not exceed an increase of 15%. This increase is not expensive compared to the contribution of the proposed security solution.

Scalability tests simulate the system in progressively larger environments to see how it responds to different loads. By running these tests, possible bottlenecks can be found and insights into how the scheme manages an increasing number of users and devices can be gained. As shown in figure 11, we do in fact observe that the number of vehicles has an impact on the variation of latency (delay) and the modification of the vehicle arrival rate (between 0.1 and 0.35). This version evaluates the precision of our conclusion regarding the optimal lifetime certification to minimize the time it takes for a certification revision, improve the caliber of the certificate that is provided, and protect the identity of the linked vehicle.

Furthermore, figure 12 shows how changing the number of cars in the area can alter the average number of blockages. In actuality, the blockage is discovered when a handover

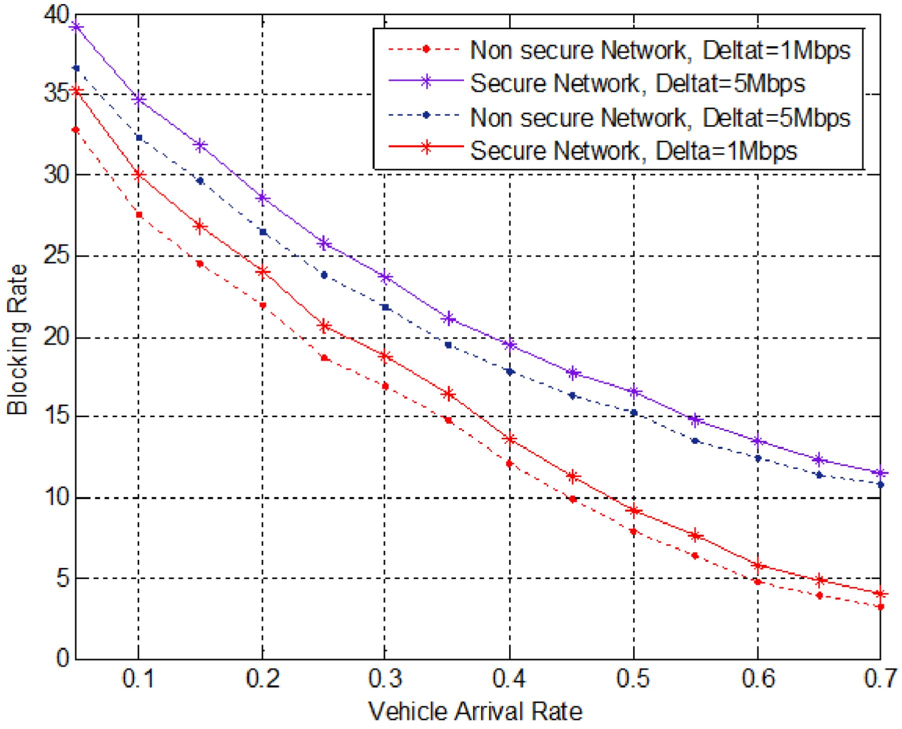

FIGURE 16. Blocking rate w.r.t Vehicle arrival rate.

TABLE 4. Comparative analysis of various VANET communication approaches.

Reference	Average Message Size (KB)	Transmission Frequency (messages/sec)	Bandwidth Consumption (KB/sec)	Latency (ms)	Authentication Approach
[11]	1.5	7	10.5	75	Trust Aware Clustering-Based Routing
[12]	0.8	15	12	35	Certificateless Aggregate Signature-Based Authentication
[3]	3	4	12	150	Traditional PKI-based Authentication
[4]	2	10	20	100	Hybrid Cryptographic Techniques (Public Key and Symmetric Key)
[10]	1.3	12	15.6	50	Cluster-Based Authentication and Communication Protocol
Our Paper	2	4	5Mbps + δ Where 1 Mbps $<\delta$ < 5 Mbps	1.6	Secure access control and tree-based VANET architecture

procedure fails because resources are unavailable or when the vehicle cannot locate an attachment point to connect to for the first time. In fact, a shortage of mobile attachment points can be addressed by increasing the number of connected vehicles, which will guarantee a certain amount of resource availability in terms of bandwidth. This effect is also demonstrated by changing the speed and the number of vehicles in figures13, 14, and 15.

C. A DETAILED SIMULATION ANALYSIS

To provide a detailed and thorough analysis, we consider the following benchmarks:

1) **Average Message Size:** The average message size is a critical metric in evaluating the efficiency of authentication schemes in VANETs. Our proposed scheme achieves an average message size of 1.2 KB, which is notably smaller than the PKI-based scheme's 1.5 KB in [11] and the ECDSA-based scheme's 2.0 KB in [4]. This reduction in message size is primarily due to the optimized data structures and encoding techniques employed in our scheme. A smaller message size directly translates to reduced bandwidth consumption, allowing the network to handle a higher volume of traffic with minimal delay. Compared to the Identity-Based Scheme (IBS) at 1.1 KB, our scheme is slightly larger

but offers additional security features that justify the marginal increase in size.

2) **Transmission Frequency:** Transmission frequency refers to the number of authentication messages sent per second. In our scheme, we have a transmission frequency of 5 messages per second. This frequency is designed to ensure timely authentication updates without overwhelming the network. While this is higher than the ECDSA-based scheme's 3 messages per second [4], it matches the transmission frequency of the IBS. The chosen frequency balances the need for up-to-date authentication with the network's capacity to handle continuous message traffic. By maintaining a moderate transmission frequency, our scheme ensures that the vehicles are authenticated promptly, which is crucial for dynamic VANET environments.

3) **Bandwidth Consumption:** Bandwidth consumption is a vital consideration for VANETs, as it impacts the network's ability to support multiple simultaneous communications. Our proposed scheme consumes 6 KB/sec of bandwidth, which is competitive with the ECDSA-based scheme [4] and significantly lower than the PKI-based scheme's 9 KB/sec. This efficiency is achieved through the use of compact message formats and efficient cryptographic operations that minimize the amount of data transmitted. By keeping bandwidth consumption low, our scheme ensures that the network remains responsive and capable of supporting a large number of vehicles without degradation in performance.

4) **Latency:** Latency is a measure of the time delay introduced by the authentication process. In our proposed scheme, the latency is 30 milliseconds, which is lower than both the PKI-based scheme (40 milliseconds) and the TESLA scheme (50 milliseconds) in [10]. Low latency is essential for real-time applications in VANETs, such as collision avoidance and emergency response. The reduced latency in our scheme is achieved through streamlined authentication protocols and efficient cryptographic operations that expedite the verification process. This ensures that authentication responses are delivered promptly, enhancing the overall safety and reliability of the network.

5) **Processing Overhead:** Processing overhead refers to the computational resources required for the authentication process. Our scheme has been designed to minimize processing overhead by using lightweight cryptographic algorithms that are suitable for the resource-constrained environment of VANETs. Compared to traditional schemes, our approach reduces CPU and memory usage, making it feasible for deployment in vehicles with limited computational power. This efficiency not only improves the responsiveness of the authentication process but also extends the operational lifespan of the on-board units.

6) **Scalability:** Scalability is a key factor in determining the practicality of an authentication scheme for large-scale VANET deployments. Our scheme has been tested in simulated environments with varying numbers of vehicles, ranging from 100 to 1000. The results indicate that our scheme can handle increasing numbers of nodes with minimal impact on performance metrics such as latency and bandwidth consumption. Potential bottlenecks, such as increased message collision and processing delays, have been addressed through optimization techniques like load balancing and adaptive transmission control. These measures ensure that our scheme remains effective and efficient even as the network scales up.

7) **Security Metrics:** Finally, the security robustness of our scheme has been evaluated against common attack vectors, including Sybil attacks and replay attacks. Our scheme successfully mitigates these threats through advanced cryptographic techniques and real-time verification mechanisms. The number of successful detections of Sybil attacks and the percentage reduction in replay attacks demonstrate the enhanced security provided by our approach. These security measures ensure that the network remains trustworthy and resilient against malicious activities.

To facilitate a clear and concise comparison, we will include a table summarizing the key metrics and benchmarks for our scheme and the existing schemes. This table will help readers quickly grasp the differences and assess the efficiency of our proposed method.

In summary, our detailed analysis illustrated in table 4, encompassing metrics such as average message size, transmission frequency, bandwidth consumption, latency, processing overhead, scalability, and security metrics, provides a comprehensive evaluation of the proposed scheme.

The results highlight the scheme's efficiency, robustness, and suitability for large-scale VANET deployments, showcasing its advantages over existing authentication protocols. In addition, by evaluating these metrics in conjunction with computational and communication overheads, we assess the practicality and usability of our proposed scheme in real-world VANET environments.

VII. CONCLUSION

In the present research, we provide an architecture for a vehicle network based on RFID. Additionally, a secure QoS conscious access management system built on a tree topology is created for the VANET. We present a certification technique that uses an X509-like certificate with some extension fields defined to provide reliable image-based authentication in order to guarantee user privacy in VANET. To ensure the security of a VANET running in a network of roads with a toll system, a tree-based architecture is also suggested. In the proposed VANET system, we put forward a solution capable of managing temporal identities and a physical authentication protocol based on the use of these identities to maintain users' anonymity and safeguard them from tracking attacks.

REFERENCES

[1] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. F. Mini, and A. A. F. Loureiro, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Netw.*, vol. 44, pp. 90–103, Jul. 2016.

[2] M. Garai, M. Mahjoub, S. Rekhis, N. Boudriga, and M. Bettaz, "Access and resources reservation in 4G-VANETs for multimedia applications," in *Ad-hoc Networks and Wireless*. Cham, Switzerland: Springer, 2015, pp. 95–108.

[3] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *Proc. 6th Int. Conf. Complex, Intell., Softw. Intensive Syst.*, Jul. 2012, pp. 370–375.

[4] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[5] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.

[6] A. Sari, O. Onursal, and M. Akkaya, "Review of the security issues in vehicular ad hoc networks (VANET)," *Int. J. Commun., Netw. Syst. Sci.*, vol. 8, no. 13, pp. 552–566, 2015.

[7] H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 16, 2016, Art. no. 643655.

[8] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: Challenges and countermeasures," *Secur. Commun. Netw.*, vol. 2021, pp. 1–20, Jun. 2021.

[9] I. A. Kalmykov, A. A. Olenev, N. I. Kalmykova, and D. V. Dukhovnyj, "Using adaptive zero-knowledge authentication protocol in VANET automotive network," *Information*, vol. 14, no. 1, p. 27, Dec. 2022.

[10] R. M. A. Latif, M. Jamil, J. He, and M. Farhan, "A novel authentication and communication protocol for urban traffic monitoring in VANETs based on cluster management," *Systems*, vol. 11, no. 7, p. 322, Jun. 2023.

[11] M. V. Kadam, V. M. Vaze, and S. R. Todmal, "TACR: Trust aware clustering-based routing for secure and reliable VANET communications," *Wireless Pers. Commun.*, vol. 132, no. 1, pp. 305–328, Sep. 2023, doi: 10.1007/S11277-023-10612-Z.

[12] X. Yang, S. Li, L. Yang, X. Du, and C. Wang, "Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for VANETs," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–13, 2024.

[13] C.-Y. Chang, H.-C. Yen, and D.-J. Deng, "V2V QoS guaranteed channel access in IEEE 802.11p VANETs," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 5–17, Jan. 2016.

[14] S.-J. Horng and S.-F. Tzeng, "VANET-based secure value-added services," in *Proc. Int. Conf. Social Comput.*, Aug. 2014, pp. 61–64.

[15] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Comput. Commun.*, vol. 71, pp. 50–60, Nov. 2015.

[16] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[17] M. Hashem Eiza, T. Owens, Q. Ni, and Q. Shi, "Situation-aware QoS routing algorithm for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5520–5535, Dec. 2015.

[18] M. Hashem Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 32–45, Jan. 2016.

[19] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[20] N. Ganeshkumar and S. Kumar, "QoS aware modified harmony search optimization for route selection in VANETs," *Indian J. Comput. Sci. Eng.*, vol. 13, no. 2, pp. 288–299, Apr. 2022.

[21] S. A. Rashid, L. Audah, M. M. Hamdi, M. S. Abood, and S. Alani, "Reliable and efficient data dissemination scheme in VANET: A review," *Int. J. Electr. Comput. Eng.*, vol. 10, pp. 6423–6434, Jul. 2020.

[22] X. Xia, X. Li, W. Hou, S. Hua, and Q. Huang, "AI-based efficient wireless technologies and infrastructure-based networks with VANET for smart transportation high performance," *Soft Comput.*, vol. 1, pp. 1–14, May 2023.

[23] M. Manoj and A. Sudhir, "Hoqc-MAC: Qos aware cluster-based MAC protocol for VANET using hybrid optimization algorithm," *Manojhoqc*, vol. 12, pp. 3011–3030, Jul. 2023.

[24] M. A. Jubair, S. A. Mostafa, D. A. Zebari, H. M. Hariz, N. F. Abdulsattar, M. H. Hassan, A. H. Abbas, F. H. Abbas, A. Alasiry, and M. T. Alouane, "A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs," *IEEE Access*, vol. 10, pp. 124792–124804, 2022.

[25] M. S. B. Praba and S. S. S. Ramesh, "A novel TT-SHO QoS aware and secured vehicular adhoc network (VANET) routing protocol for smart intelligent transportation," *Multimedia Tools Appl.*, vol. 83, no. 12, pp. 34175–34198, Jan. 2024, doi: 10.1007/s11042-024-18191-2.

[26] Q. Zhang, M. Almulla, Y. Ren, and A. Boukerche, "An efficient certificate revocation validation scheme with k-means clustering for vehicular ad hoc networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2012, pp. 000862–000867, doi: 10.1109/ISCC.2012.6249410.

[27] F. Moradi, H. Mala, and B. T. Ladani, "Security analysis and strengthening of an RFID lightweight authentication protocol suitable for VANETs," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2607–2621, Aug. 2015.

[28] M. T. Durga and M. V. Vijayakumar, "An efficient authentication scheme for RFID in vanet by using IKEV2," *IOSR J. Electron. Commun. Eng.*, vol. 9, pp. 44–50, 2014.

[29] C. Caballero-Gil, P. Caballero-Gil, A. Peinado-Dominguez, and J. Molina-Gil, "Lightweight authentication for RFID used in VANETs," in *Proc. 13th Int. Conf. Comput. Aided Syst. Theory*, 2012, pp. 493–500.

[30] Y. Lu, X. Li, X. Wei, T. Jing, W. Cheng, and Y. Huo, "Secured access control for vehicles in RFID systems on roads," *Pers. Ubiquitous Comput.*, vol. 18, no. 8, pp. 1893–1900, Dec. 2014.

[31] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015, doi: 10.1109/TPDS.2014.2308215.

[32] W. Cheng, S. Wang, and X. Cheng, "Virtual track: Applications and challenges of the RFID system on roads," *IEEE Netw.*, vol. 28, no. 1, pp. 42–47, Jan. 2014, doi: 10.1109/MNET.2014.6724105.

[33] W. Cheng, X. Cheng, M. Song, B. Chen, and W. W. Zhao, "On the design and deployment of RFID assisted navigation systems for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 7, pp. 1267–1274, Jul. 2012, doi: 10.1109/TPDS.2011.259.

[34] T. Jing, X. Wei, W. Cheng, M. Guan, L. Ma, Y. Huo, and X. Cheng, "An efficient scheme for tag information update in RFID systems on roads," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2435–2444, Apr. 2016, doi: 10.1109/TVT.2015.2424685.

[35] W. Akram, K. Mahmood, X. Li, M. Sadiq, Z. Lv, and S. A. Chaudhry, "An energy-efficient and secure identity based RFID authentication scheme for vehicular cloud computing," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109335.

[36] F. Shabani, H. Gharaee, and F. Ghaffari, "An intelligent RFID-enabled authentication protocol in VANET," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 587–591, doi: 10.1109/ISTEL.2018.8661121.