future internet

MDPI

Article

Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET

Nishu Gupta [1,*], Ravikanti Manaswini [1], Bongaram Saikrishna [1] and Francisco Silva [2,*] and Ariel Teles [3]

[1] Electronics and Communication Engineering Department, Vaagdevi College of Engineering, Warangal 506005, India; manaswini13.mr@gmail.com (R.M.); gopalakrishna9154@outlook.com (B.S.)
[2] Computer Science Department, Federal University of Maranhão, São Luís 65080-805, Brazil
[3] Campus Araioses, Federal Institute of Maranhão, Araioses 65570-000, Brazil; ariel.teles@ifma.edu.br
* Correspondence: nishugupta@ieee.org (N.G.); fssilva@lsdi.ufma.br (F.S.); Tel.: +91-96-5150-8346 (N.G.)

Received: 5 March 2020; Accepted: 30 March 2020; Published: 1 April 2020

Abstract: The amalgamation of Vehicular Ad hoc Network (VANET) with the Internet of Things (IoT) leads to the concept of the Internet of Vehicles (IoV). IoV forms a solid backbone for Intelligent Transportation Systems (ITS), which paves the way for technologies that better explain about traffic efficiency and their management applications. IoV architecture is seen as a big player in different areas such as the automobile industry, research organizations, smart cities and intelligent transportation for various commercial and scientific applications. However, as VANET is vulnerable to various types of security attacks, the IoV structure should ensure security and efficient performance for vehicular communications. To address these issues, in this article, an authentication-based protocol (A-MAC) for smart vehicular communication is proposed along with a novel framework towards an IoV architecture model. The scheme requires hash operations and uses cryptographic concepts to transfer messages between vehicles to maintain the required security. Performance evaluation helps analyzing its strength in withstanding various types of security attacks. Simulation results demonstrate that A-MAC outshines other protocols in terms of communication cost, execution time, storage cost, and overhead.

Keywords: authentication; internet of vehicles; intelligent transportation systems; security; vehicular Ad hoc networks

1. Introduction

By 2020, around 50 billion devices will be connected to the Internet for a better society using different technological systems. The concept of smart objects which provide seamless connectivity along with ensuring safety and a smart environment through increasing interaction and interoperability is called the Internet of Things (IoT) [1]. Vehicle users enjoy a better experience when amalgamating the IoT and Vehicular Ad hoc Network (VANET) architectures, and this emerging field is called the Internet of Vehicles (IoV) [2]. With the exponential development of big data and IoT concepts, IoV has become one of the key enablers to realize future autonomous driving scenarios and ad hoc networking technologies. In the current research paradigm about Intelligent Transportation Systems (ITS), conventional VANET is transforming into IoV. VANET is a subclass of Mobile Ad hoc Network (MANET) and a component of ITS that provides two types of communications: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [3]. It is designed to exchange vital information using dedicated short-range communication (DSRC) standard on the road [4]. It is used in safety and non-safety applications such as present location, traffic, road safety, and driver assistance/comfort [5,6].

The increase in the number of vehicles has led to rising traffic congestion and frequent traffic accidents. Therefore, there is a need to improve driving experience and enhance driver safety. This has

led to the research of enhancing driver safety [7]. The typical structure of VANETs comprises three parts: a Trust Authority (TA), a Roadside Unit (RSU), and an On-Board Unit (OBU). The TA, which acts as the trusted management center, is responsible for the registration and issuing of secret key material. The RSU, installed along the roads, serves as a bridge between the vehicles and the TA [8].

Despite numerous advantages of VANETs, there are still some challenges that need to be solved [9–11]. Since messages are transmitted in an open wireless environment, a robust security protection mechanism is required. Moreover, requirements for fast authentication and privacy protection must be ensured [12]. Another significant requirement of VANET is to ensure and enhance safety. This requires effective and trustworthy transmission of messages among vehicles. However, being operational in an insecure environment, it is susceptible to malware attacks. In general, VANETs should be able to ensure privacy, security and reliability of messages while accomplishing efficient authentication, as well as resisting security attacks. To address such issues, an Authentication-based Medium Access Control (A-MAC) protocol is proposed in this article. To the best of our knowledge, this is the first authentication-based secure data dissemination protocol for 5G-enabled vehicular communications. In this paper, we have made the encryption algorithm lightweight by introducing a smaller number of variable parameters to reduce the storage space. Moreover, it helps achieve secure message authentication with lower computation overhead. Major contributions of this article are:

1. An interactive framework for various levels in IoV Architecture is presented;
2. Secure message authentication protocol is designed for 5G-enabled vehicular networks;
3. Performance evaluation is conducted and a comparison with other protocols is performed.

The proposed work is not only an extension of solution to Media Access Control (MAC) layer issues but also gives a detailed explanation to the layers of IoV architectural model.

Figure 1 depicts a model of a vehicular scenario. It is also helpful in supplying abounding multimedia and mobile Internet application services. IoV has convergent concentration as serving application of ITS by ensuring driver safety, traffic efficiency and infotainment. IoV service is needed by smart cities for big scale data sensing, collection, information, processing and storage. One of the main challenges of the IoV deployment in the smart cities is integration of all its components. Another challenge is to ensure reliable and real-time delivery of rapid emergency services and big scale of data collection between vehicular application and platform [5].

The rest of this article is structured as follows. In Section 2, we first present the related works. Section 3 presents the interactive model and architecture of IoV. Section 4 presents the system model and the proposed protocol aiming to enhance user experience and performance of traffic system. In Section 5 we simulate the presented protocol and evaluate its performance to prove its effectiveness. We compare the performance of various existing schemes with the proposed scheme. Finally, we discuss future scope related with the implementation of IoV. Finally, we discuss future scope related with the implementation of IoV in Section 6 and draw our conclusions.

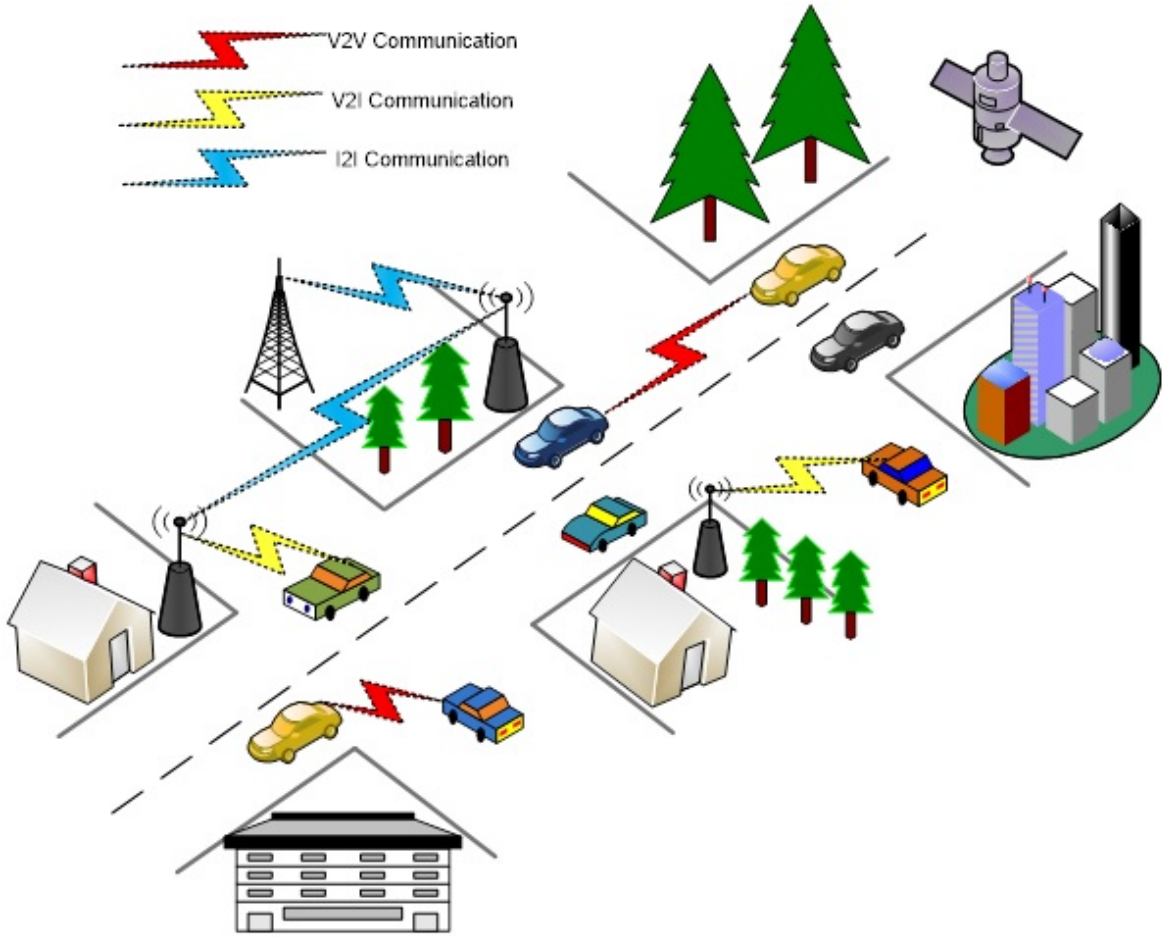

Figure 1. A model of vehicular scenario.

2. Related Work

Rapid emergence of ITS-based technologies has attracted researcher's attention towards communication between vehicles as road safety and development of transportation efficiency [13]. Specifically, for a long time, VANET has been under the spotlight for this purpose [14].

VANET uses DSRC technologies [5,15]. However, it has its own limitations such as dynamic topology and intermittent network connectivity [5]. The problem remains unsolved due to high-speed mobility of vehicle and currently incomplete infrastructure, leading to reliability of services and connection in VANET being vulnerable.

IoV architecture was first proposed in [16] but it had limited communication facility. Little later, researchers in [17] came up with five-layered architecture comprising different communications such as V2V, V2I, Vehicle-to-Roadside Unit (V2R), Vehicle-to-Sensors (V2S), Vehicle-to-Personal devices (V2P), and Vehicle-to-Mobile station (V2M). However, both these IoV layered structures did not discuss possible security issues. Various researchers in [18–21] progressed in ensuring privacy in VANETs. However, the security in these schemes depend only on the private key of the trust authority which could lead to security flaws. The authors in [22] suggested a dual authentication and key management method using the hash code and biometric identity to avoid malicious users to use the secret key for VANET applicants. However, the scheme finds limited applicability in the way that intruders can track the vehicles' location. In [8], authors proposed a message authentication protocol to improve performance results in VANETs, but the execution cost is high, and this scheme is vulnerable to impersonation, man-in-the middle, illusion, modification, and plain-text attacks. Ultimately, most of

these protocols need high execution time, communication overhead, and storage cost. Thus, these schemes consume more energy during the implementation.

Under agreed communication protocol and data interaction, standards, wireless communication, and exchange information are conducted for IoV between vehicle-to-anything (V2X) such as another vehicle and road infrastructure [3]. The authors in [23] proposed a risk driven authentication approach dependent on discrete events. It used Petri networks to execute the validation, which lead to further increased in communication overhead. The investigation of [24] proposed a technique for using Rivest–Shamir–Adleman (RSA) encryption and Message-Digest algorithm 5 (MD5) hash capacity to encode information before transferring it on a cloud domain to keep up its information security. Their plan leveraged the use of RSA to scramble information and hash functions are determined using MD5 cryptographic hash capacities. In addition, authors in [25] proposed a safe hashing capacity which creates a variable length of 128, 160, 192, 224, or 256 bits at the output. Their investigation holds the underlying information square of 512 bits together with the original compression function for preparing its inward activities. The authors in [26] proposed another technique to improve the security of the hashed passwords by using the 6 bits saved in a transmission control protocol (TCP) whenever this Message-Digest value is being sent over a medium.

In [27] a batch verification scheme for IoV is proposed to reduce the message verification time, but it takes a high amount of time to authenticate the messages at the receiver side because it uses high-cost operations in the message confirmation scheme. In most of the proposed schemes, the verification process is carried out through batch verification of signatures. In batch verification, the recipient of the messages verifies multiple signatures simultaneously, rather than sequentially.

From the literature review, we understand that most of the schemes are vulnerable to various threats. To the best of our knowledge, an exhaustive secure communication system such as the one presented in this article to provide all five types of interactive levels for the IoV framework has not been designed before. In Table 1, we summarize the security and performance requirements fulfilled by the authentication and privacy schemes discussed above.

Table 1. Features of authentication-based schemes.

Scheme	Overhead	Source Auth.	Modification	Privacy	Loc. Track	ID Disclosure	Traceability
[8]	High	✓	✓	✓	✗	✓	✗
[18]	High	✓	✓	✓	✗	✓	✓
[19]	Low	✓	✓	✓	✗	✗	✓
[20]	✗	✓	✓	✓	✗	✓	✓
[21]	Low	✓	✓	✓	✗	✓	✓
[22]	Low	✓	✓	✓	✓	✓	✓
[23]	High	✓	✓	✓	✓	✗	✗
[24]	Medium	✓	✓	✓	✗	✓	✓
[25]	Medium	✓	✓	✓	✓	✓	✓

3. Interactive Model and Architecture of IoV

IoV mainly focuses on the integration of human and vehicle which is an extension of human abilities. It is a network model, service model and behavior model of the human-vehicle interaction system which is highly different from the wireless mobile network [28]. IoV applications can be comprehensively characterized into two different ways, safety and non-safety. For example, non-safety applications incorporate vehicle sharing, gaming, infotainment, and map download. Safety applications are, for example, route, remote telematics, indicative, traffic proficiency, co-usable message move, post-crash warning, upgrading traffic well-being, participate to support different vehicles, and ongoing traffic.

3.1. Interactive Model

One of the key highlights of the IoV is its interactive model (Figure 2) that includes V2V [29–31], V2R [32], V2S, V2M, and V2I. The IoV implementation requires different devices such as vehicles, portable gadgets, RSUs, sensors, and actuators, to serve as fundamental necessity for ITS applications. For these communication systems, Data Acquisition System (DAS) is required where the vehicular data is transferred on the network through on road diagnosis interface. It helps in avoiding accidents, renders safety driving and improves driving experience [33]. Figure 2 shows the layout of an immediate connection between these gadgets and the IoV server. The registration and authentication processes are conducted through a secure link such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) convention [12,18,34].

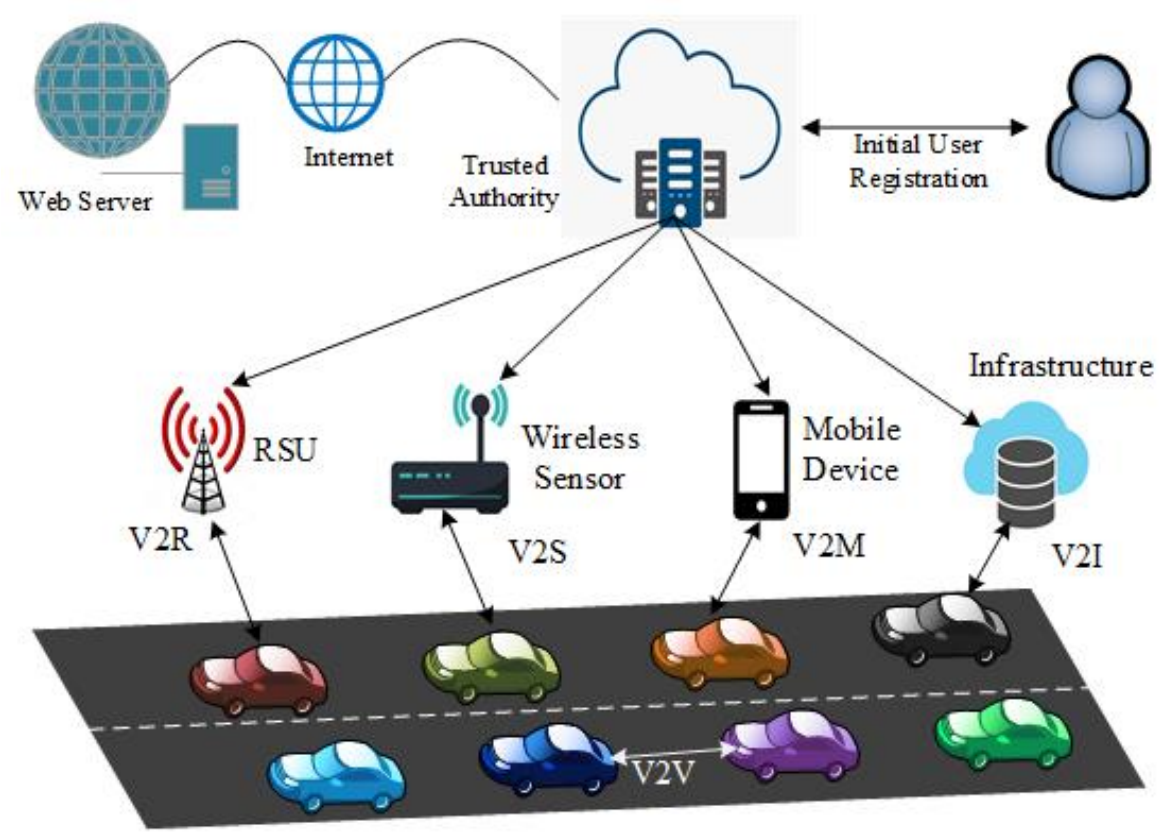

Figure 2. An interactive model of IoV.

3.2. IoV Architecture

Based on the existing architecture of IoV which is observed to have some of inherent issues, we propose a five-layered IoV architecture namely Sensing layer, Communication layer, Control layer, Cognition layer, and Application layer as shown in Figure 3.

3.2.1. Application Layer

At the application layer, basically three types of IoV application platforms are supported viz. service management, public information, and early warning monitoring and decision. These ones are classified broadly under customized applications and intelligent transportation applications. These services are opportunistic in nature as they are dynamic, context-aware and co-located [35]. The customized application is to reduce safety risks during driving whereas intelligent transportation applications include, for example, traffic management, safe driving, and smart alerts.

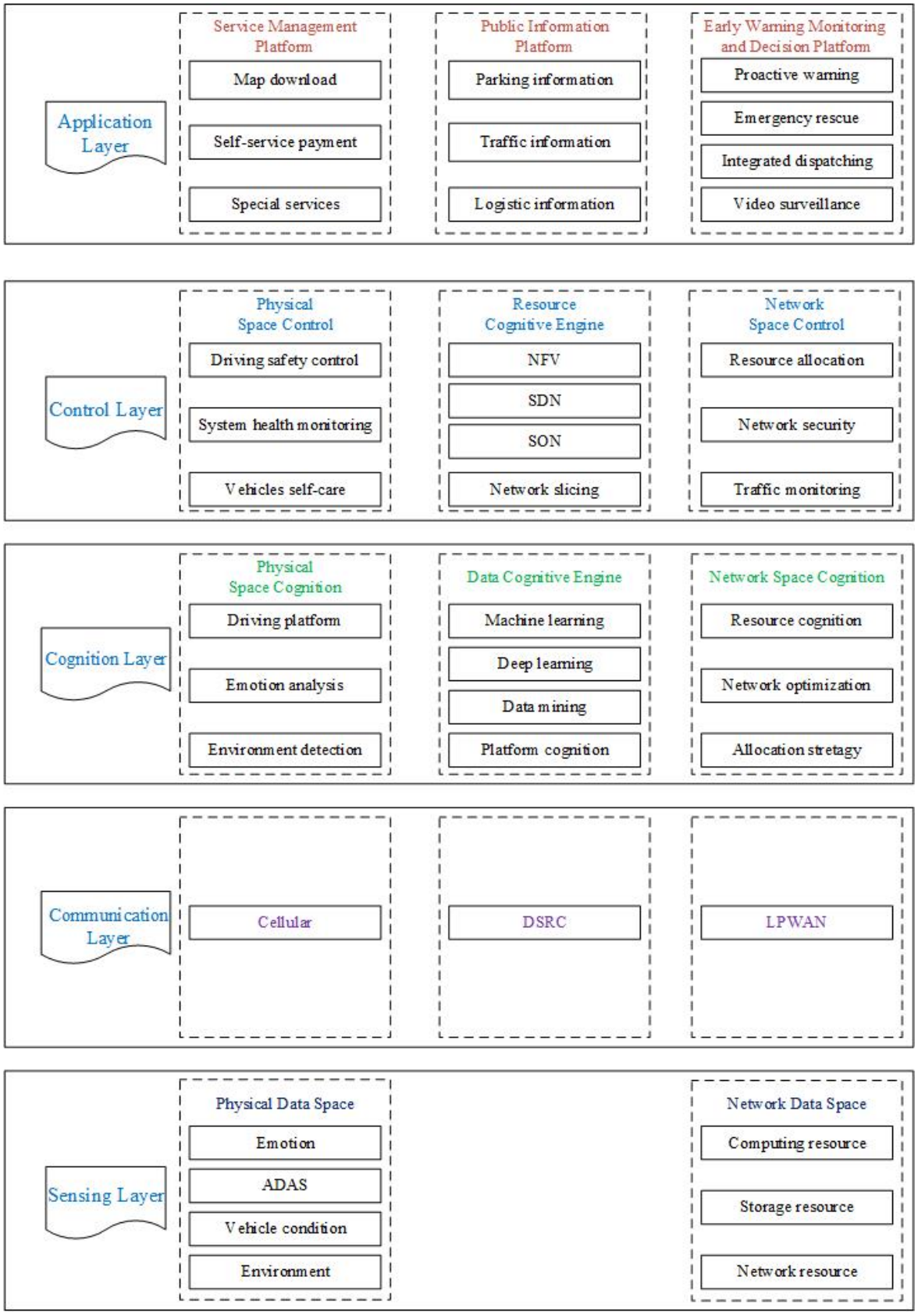

Figure 3. Proposed architecture of IoV.

3.2.2. Control Layer

In the control layer, cognitive engines are employed to reinforce the permanency and dependability in the network and to meet Quality of Service (QoS) necessities of intra-vehicle applications. The resource of intra-vehicle is reliable for the actual processing of driving data. In this, speediest decision-making can be secured. Resource organized on cloud perform network optimization in a centralized system all through efficient deployment of the global intelligence of IoV. Implementation on cloud is at the price of large integrated data storage, processing and bandwidth resources. In particular, the major work of cloud is to observe resource deployment on edge network and to perform dynamic scheduling for resources in actual time. In addition, cloud receives developing messages sent by edge and performs a sequence of emergency treatment through high-performance computing.

3.2.3. Cognition Layer

A cognitive engine relates to a physical data space and the cognition layer divides into cognition and resource cognitive engines at the control layer. The data cognitive engine processes and analyzes data flows using, for example, machine and deep learning techniques, data mining, and pattern recognition with complex event processing [36]. In network space, the data cognitive engine sends data analysis results to resources cognitive engine to guide network resource allocation. The vehicle areas are deployed to edge unit and non-vehicle areas are deployed to cloud unit. In network data space, the data cognitive engine can realize dynamic cognition of data such as computing, storage, and network resources. If there is any delay in a specific task, then the edge will check whether it can complete or not [15].

3.2.4. Communication Layer

Communication layer is mostly accepted in cloud/edge hybrid architecture. It is associated with the wireless communication layer (such as Wi-Fi, DSRC, LTE). For the most part of driving data, the intra-vehicular network requires reasonable local dispensation and computing using the actual-time communication among intelligent devices on the cloud. The major purpose of this layer is resource optimization. The actual-time data communication can be recognized across self-establishing network among vehicles and RSUs. At significant level, the cloud's requirement is to perform centralized control across the entire traffic information, and to authenticate the feature model for network topology, road situation information and space-time service of autonomous moving pieces of the entire IoV.

3.2.5. Sensing Layer

This layer is responsible for the sensing of objects to collect the data from multi-data operators. Data can be collected in form of details about vehicles and RSUs, and these systems are interlinked with cloud server to give information about the vehicle's location. In this process, edge/cloud devices are used. Sensing layer is also used for cleaning and normalizing the data [37]. Physical data space takes care of driving pattern and leverages, for example, Advance Driver Assistance System (ADAS), behavior pattern, and emotions.

As a new technology, 5G is characterized by high speed, low delay, wide coverage and support for Device-to-Device (D2D) communications, IoV creates a huge opportunity for further enhancements and performance improvements in VANET [38,39]. When compared with traditional sensor network, there are higher requirements on perception accuracy, stability in data transmission, real-time analysis, intelligent decisions and network reliability for IoV, demanding for more complex architectures. For that reason, the proposed architecture meets the requirements of IoV, comprising application layer, control layer, cognition layer, communication layer and sensing layer as shown in Figure 3.

4. System Model for A-MAC

In the system model, we consider a network of distributed vehicles, following Distributed Coordination Function (DCF) mechanism. We consider a twin-layer network scenario comprising vehicles and TAs. It is assumed that TAs are fully authenticated and are a part of DCF. Each TA is assigned a network region and is responsible for vehicle registration and generating various system parameters in the network. It is assumed that all vehicles in a network are equipped with an OBU which renders data transmission and reception. Moreover, each vehicle is equipped with a device which is used to store encrypted data. Table 2 shows the main notations and their corresponding meanings.

Table 2. The notation and specific descriptions.

Notations	Description
ϱ_1	Any vehicle x in the network
TA	Trust Authority
ID_{TA}	ID of TA
ID_{ϱ_1}	ID of any vehicle x
θ_{TA}	Private key of unit TA
$h(.)$	Hash function
$\oplus$	XOR operator
$\parallel$	Connection symbol

In the below sections, we define and explain A-MAC protocol to reach inconsequential certification of V2V communication. According to this protocol, only authenticated vehicles are permitted to disseminate messages among each other. The protocol is further subdivided into three sub-protocols namely initiation level, assessment level, and validation level.

4.1. Initiation Level

In the A-MAC authentication protocol, each node (we address vehicle and node intermittently) in the region of TA is uniquely identified with an ID. TA generates specific privacy key using security single hash function $h(.)$ as given in the equation below

$$\theta_{TA} = h(ID_{TA} \parallel R_{TA}) \tag{1}$$

where θ_{TA} is the privacy key to TA and ID_{TA} corresponds to the ID of TA. R_{TA} is the random number generated through the TA. It requires inputting a message of random length and the output message is 128-bit process. MD5 [40] is used to allocate the input message hooked on blocks by 512-bits. Each block is divided into 16 sub-blocks along with 32-bits. In the sequence of processing, the output obtained is four groups of 32-bits each. The four groups are cascaded and hash values through 128-bits are created. Nevertheless, the performance time of MD5 algorithm is better in all respects and execution time is 6 µs.

4.2. Assessment Level

In A-MAC, there is a provision of unique identification and security key corresponding to each vehicle. Let ID_{ϱ_0} correspond to ID of the vehicles ϱ_0 and S_{ϱ_0} correspond to security key of the vehicles ϱ_0. Instead of vehicle's id being regenerated repeatedly by the system, factors are generated using ID_{ϱ_0} and S_{ϱ_0} as shown in the following Equation.

$$\rho_{\varrho_0} = h(ID_{\varrho_0} \parallel S_{\varrho_0}) \tag{2}$$

The vehicle ϱ_0 compute the factors ζ_{ϱ_0} as shown in the following Equation.

$$\zeta_{\varrho_0} = A_{\varrho_0} \oplus B_{\zeta_{\varrho_0}} \tag{3}$$

The factor ζ_{ϱ_0} is transmitted to the TA with vehicle's ϱ_0. When received, the TA generates a random number h_{TA}. The TA factor τ_{TA} is shown in the following Equation.

$$\tau_{TA} = h(\zeta_{\varrho_0} \parallel \varphi_{\varrho_0}) \oplus \theta_{TA} \tag{4}$$

where $\varphi_{\varrho_0} = h(ID_{\varrho_0} \parallel h_{TA})$. Finally, the factors θ_{TA} and h_{TA} are transmitted to the vehicles ϱ_0, as shown in Figure 4.

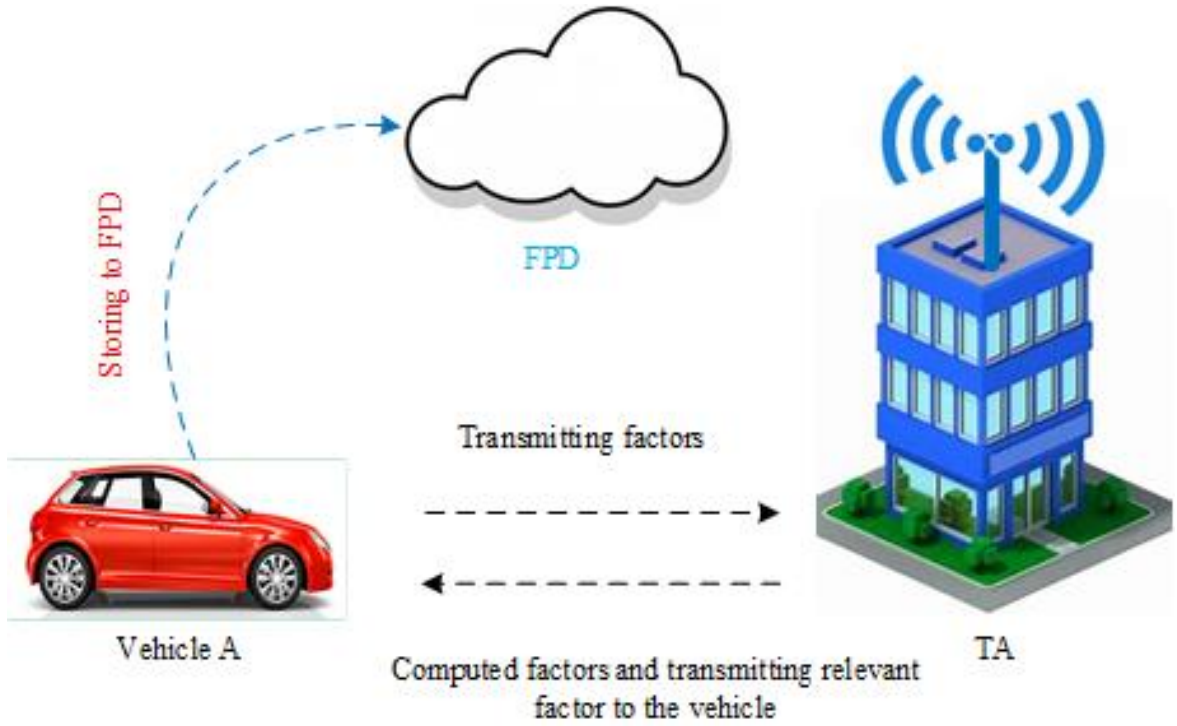

Figure 4. Vehicle authentication process in A-MAC protocol.

When a message is received, the vehicles ϱ_0 stores these factors in TA and the vehicles ϱ_0 factors $\{\zeta_{\varrho_0}, \tau_{TA}, h_{TA}, \varphi_{\varrho_0}\}$ are set accordingly.

4.3. Validation Level

Instead of communicating with others, the vehicles first authenticate their identity among themselves and then communicate with other vehicles subsequent to finishing the validation level [41]. It is further subdivided into various stages discussed below.

4.3.1. Elementary Validation

The vehicles generate the factors ζ using specific ID and security key as discussed in Equations (2) and (3). If they are identical, the vehicles are authenticated. If they are not trustworthy, they must re-register until authentication succeeds. Vehicle ϱ_0 is required to communicate with other entities, which is return factor ζ_{ϱ_0} corresponding to Equation (3). If they are equal, vehicle ϱ_0 is validated, and it is eligible to communicate with other entities. The vehicle's authorization processing is comparatively simple.

4.3.2. Message Validation

To make sure the safety of transmitting data, the communication entity is required to be validated before it is prepared to transmit data. It is again a three-step messaging process namely *request message*, *reply message* and *communication units*.

Request Message

Precisely, while vehicle ϱ_1 requests to transmit data to vehicle ϱ_2, it first sends a request message to the vehicles and marks the delivery time request. In similar fashion, vehicle ϱ_1 generates a random number h_{ϱ_2}. Subsequently, the vehicles separate the factors as of OBU and the value of factor φ_{ϱ_0} is computed. The vehicles ϱ_0 use generate factors ζ_{ϱ_0}, φ_{ϱ_0} and θ_{TA} to calculate the security key of TA, as shown in the following Equation.

$$\theta_{TA} = h(\zeta_{\varrho_0} \parallel \varphi_{\varrho_0}) \oplus \tau_{TA} \tag{5}$$

The vehicles ϱ_0 compute the following factors.

$$T_{\varrho_0} = h(\theta_{TA} \parallel S_{tx}) \oplus \zeta_{\varrho_0} \tag{6}$$

$$S_{\varrho_0} = T_{\varrho_0} \oplus \zeta_{\varrho_0} \oplus \theta_{TA} \tag{7}$$

$$\mu_{\varrho_0} = Rqst \oplus T_{\varrho_0} \oplus \theta_{TA} \oplus S_{tx} \tag{8}$$

where S_{tx} is the timestamp for the request.

Reply message

Vehicle ϱ_2 first calculates the timestamp of the received factors $\{T_{\varrho_0}, \mu_{\varrho_0} \wedge S_{tx}\}$, which is denoted as S_{rx}. Subsequently, S_{rx} is retrieved from S_{tx} which is separated from $\{T_{\varrho_0}, \mu_{\varrho_0} \wedge S_{tx}\}$.

If S_{rx} is extremely late, the following disparity must hold.

$$S_{rx} - S_{tx} \geq \alpha S_1 \tag{9}$$

where αS_1 is the system factor. While disparity holds, it has received factors $\{T_{\varrho_0}, \mu_{\varrho_0} \wedge S_{tx}\}$ are expired. Vehicle ϱ_2 is instantaneously halted communicating through vehicle ϱ_1. Then, it should go for the next step. Vehicle ϱ_2 recalculates the factors h_{ϱ_1} are provided with the help of following relations.

$$\check{h_{\varrho_1}} = T_{\varrho_0} \oplus h \tag{10}$$

Correspondingly, vehicle ϱ_2 recalculates $\check{S_{\varrho_0}}$, as shown in the following Equation.

$$\check{S_{\varrho_0}} = \check{h_{\varrho_1}} \oplus T_{\varrho_0} \oplus \theta_{TA} \tag{11}$$

Subsequently, the vehicle ϱ_2 excerpts request message from Equation (8), which is provided by the following equations.

$$Rqst = \mu_{\varrho_0} \oplus T_{\varrho_0} \oplus \theta_{TA} \oplus S_{tx} \tag{12}$$

Next, finding these factors, vehicle ϱ_2 compute two new factors F_{ϱ_2} and L_{ϱ_2} provided by the following equations.

$$F_{\varrho_2} = h(h_{\varrho_1} \parallel \alpha \check{S}_1 \parallel \theta_{TA}) \tag{13}$$

$$L_{\varrho_2} = F_{\varrho_2} \oplus \theta_{TA} \oplus \check{S_{\varrho_0}} \oplus \check{h_{\varrho_1}} \tag{14}$$

Finally, vehicle ϱ_2 communicates the applicable factors to the vehicle ϱ_1. When received, vehicle ϱ_1 sends an acknowledgement message to vehicle ϱ_2. For the security of the channel, a reply message is encoded which is provided by:

$$EN_{Reply} = ECD_{F_{\varrho_2}} \tag{15}$$

In the end, the vehicle ϱ_2 communicates factors $\{L_{\varrho_2}, Reply\}$ to the vehicles.

This protocol proposes to decrease the operation time of the authentication process. Recalling Equation (15), the pieces of data needed? to the encoder are reply messages and the key F_{ϱ_2}. Using Reply and F_{ϱ_2} as input to the protocol, the encoder EN-reply is generated.

Communication units

The exchange of control bits (sent, replay) among the vehicles enables to get each other's information. When receiving $\{L_{\varrho_2}, Reply\}$, vehicle ϱ_1 is first recorded of the data acceptance and the timestamps are represented by S_{tx}. Subsequently, vehicle ϱ_1 ensures safety check whether disparity $S_{rx} - S_{rx} \geq \alpha S_2$ is satisfied or not. If not, vehicle ϱ_2 avoids communicating with vehicle ϱ_1.

Once disparity $S_{rx} - S_{rx} \geq \alpha S_2$ is satisfied and found to be secure, vehicle ϱ_1 will get a reply message from EN-Reply. To get the reply, vehicle ϱ_1 should compute F_{ϱ_2} perfectly and decrypt it successfully. Correspondingly, vehicle ϱ_1 computes F_{ϱ_2} according to Equation (16).

Let $\check{F}_{\varrho_2}$ and F_{ϱ_2} compute vehicle ϱ_1, which is givens as:

$$\check{F}_{\varrho_2} = L_{\varrho_2} \oplus \theta_{TA} \oplus S_{\varrho_1} \oplus h_{\varrho_1} \tag{16}$$

The factor F_{ϱ_2} is used to decrypt the EN-Reply and to get the reply message successfully given as:

$$Reply = DCP_{F_{\varrho_2}}(EN - Reply) \tag{17}$$

where $DCP_{F_{\varrho_2^{(*)}}}$ is the decrypted function. If $\check{F}_{\varrho_2} = F_{\varrho_2}$ is validated, vehicle ϱ_1 can decrypt $EN - Reply$ and get the reply. When correctly decrypted, vehicle ϱ_1 deems that vehicle ϱ_2 is protected and vehicle ϱ_1 should communicate with vehicle ϱ_2.

5. Performance Evaluation

In this section, we present an evaluation of our proposed protocol based on the simulation results obtained using MATLAB (version R2015a) [42] and compare it with recent authentication-based schemes for VANETs [18–21]. We analyze the following performance metrics: communication cost, storage cost, execution time, and RSU's overhead. In the end, we discuss and summarize the obtained results.

5.1. Communication and Storage Costs

The communication cost is computed based on the total number of vehicles using different variables in the message transmission across the V2V communication area, as shown in Figures 5 and 6, for communication and storage costs, respectively. The storage cost is the overall memory required to store various factors. We are contemplated that the hash function is of 256-bit, a size of random number of 8-bytes, a timestamp is of 4 bytes, bi-linear combination of 128 bytes, symmetric and asymmetric encoder and decoder of 64 bytes, and signature of 128 bytes. Communication cost increases with increasing number of vehicles and the same is evident from the obtained results.

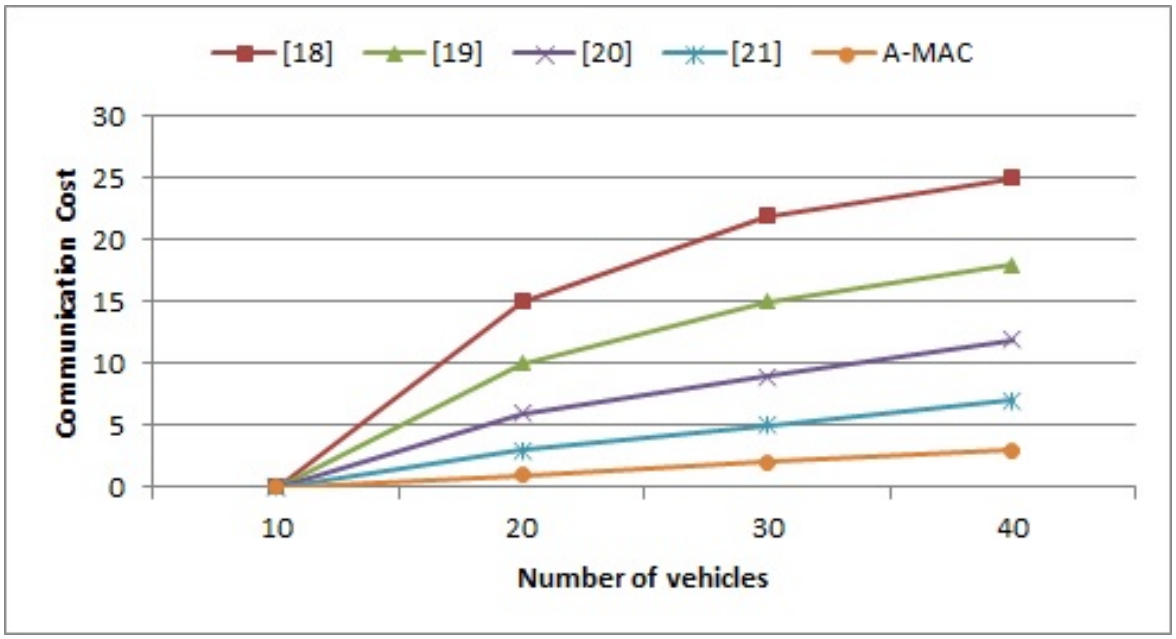

Figure 5. Communication cost.

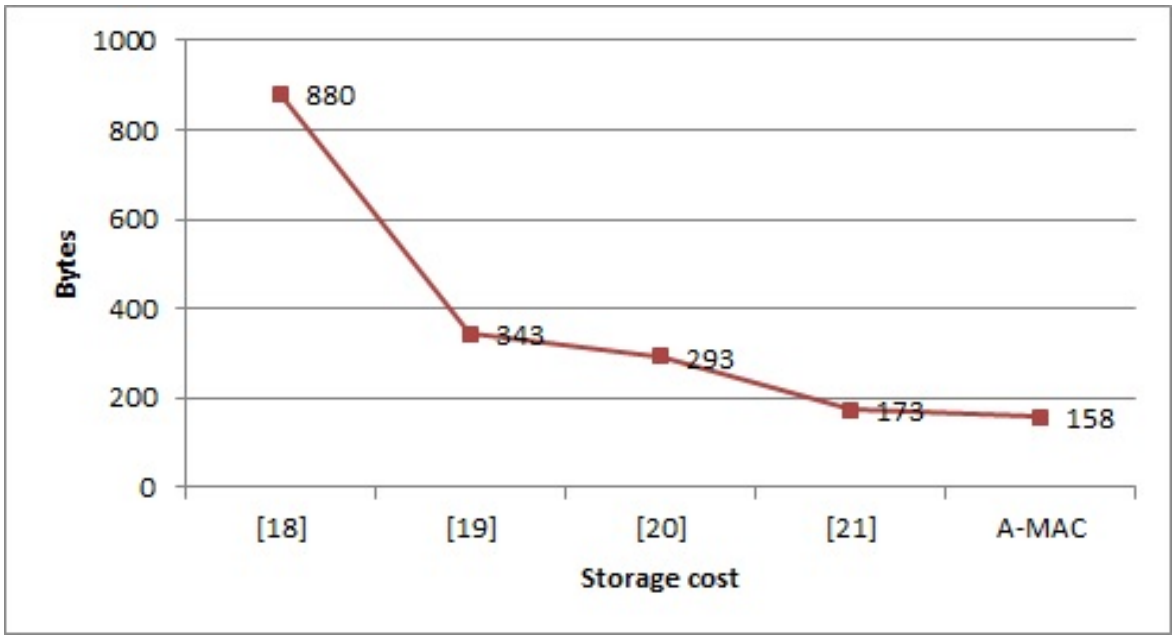

Figure 6. Storage cost.

Figure 6 shows the curve between storage cost and bytes stored. Storage cost is the amount of space required to store all the parameters. As it can be seen, storage cost is lowest for the proposed A-MAC protocol. This clearly justifies that the DCF of the A-MAC protocol is suitable for safety message dissemination under highly dense vehicular scenario. This is in line with the initial purpose for designing the protocols scheme, which decreases communication and storage costs.

5.2. Execution Time

The execution time is based on the total number of operations required for the authentication process. Figure 7 depicts the execution time comparison between A-MAC protocol and the existing protocols. It can be seen that the execution time is lesser in case of the proposed

protocol. This improvement is attributed to the cause that A-MAC relies upon relaying (multi-hop) message delivery.

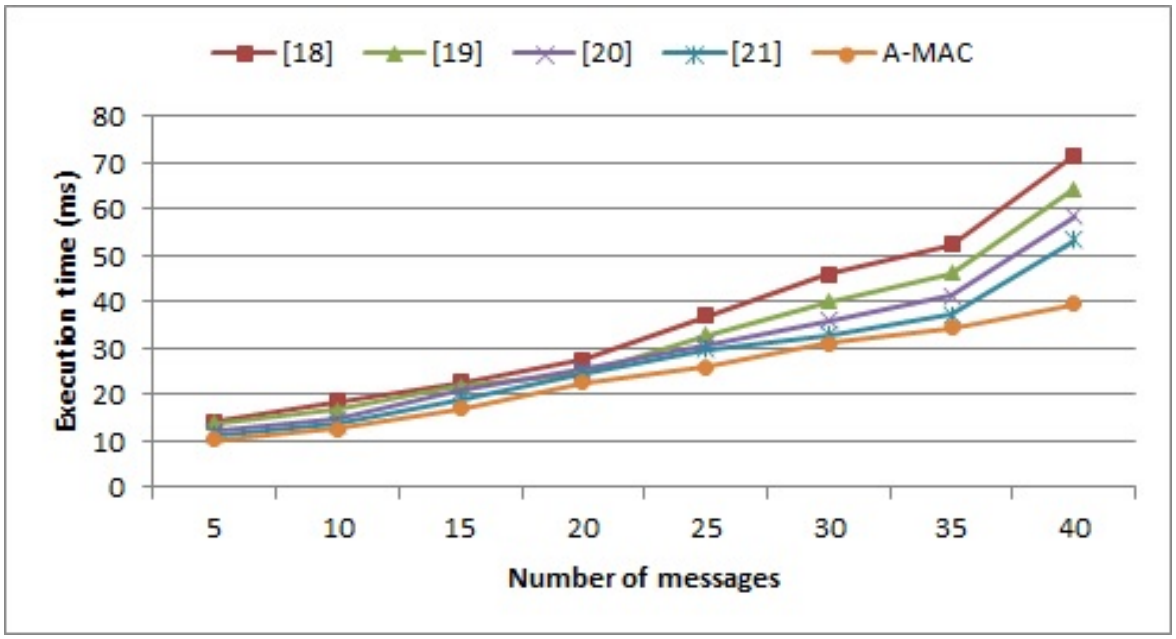

Figure 7. Execution time.

5.3. RSU's Overhead

In our proposed scheme, the message authentication task is assigned to the RSU. It is assumed that each vehicle sends only one message in the 300ms as specified by DSRC. It can be seen in Figure 8 that the overhead of our scheme is better than other schemes when the system does not have any invalid signature and when all message authentication overheads are assumed to be within one RSU's domain.

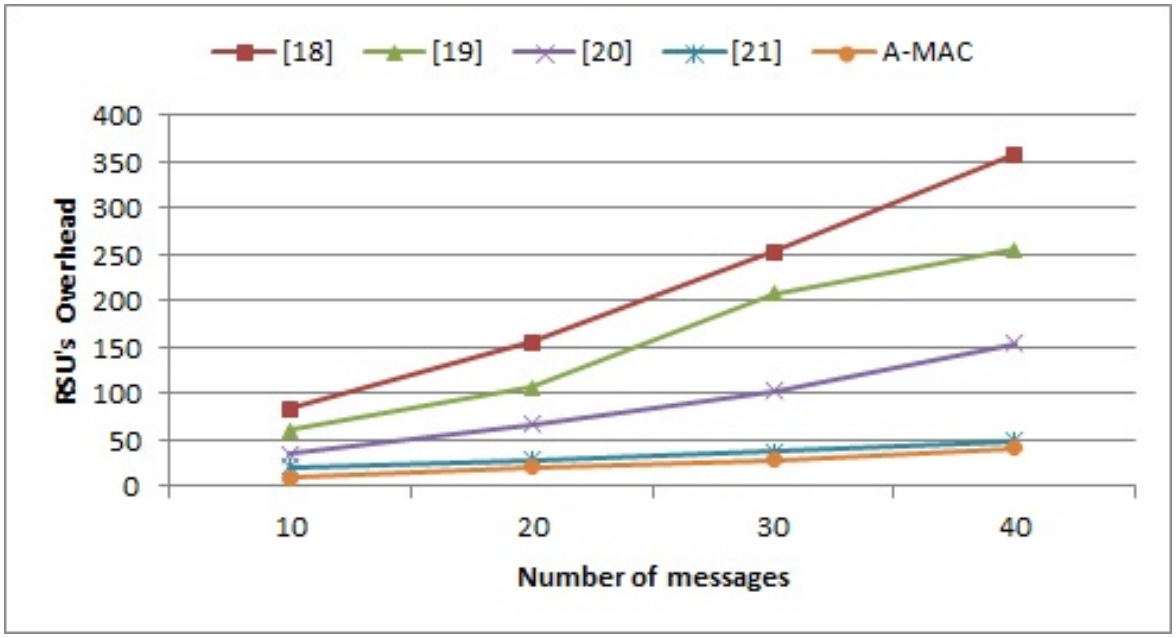

Figure 8. RSU's Overhead.

5.4. Discussion and Comparative Summary

Sensor nodes are noticed to work smartly and collect information from the surroundings. However, they are constrained with their resources such as processor, memory, and battery life. Therefore, security provisioning becomes a difficult task due to restricted resources.

As long as RSU is equipped with a modern CPU, the computation overhead of the proposed scheme will be negligible for RSU. However, in absence of such a unit, it may rise invariably. The security analysis of our scheme shows that it is more efficient in meeting more functional requirements. Hence, the proposed scheme can be implemented to exchange relevant information rapidly between vehicles directly for smart city applications.

To summarize, we tabulate the performance of different schemes along with the proposed scheme in Table 3. It is observed that the proposed protocol gives optimum performance under the defined scenario and assumptions being made.

Table 3. Summary of performance of various schemes under comparison.

Metric	[18]	[19]	[20]	[21]	A-MAC
Communication cost	High	High	Medium	Low	Low
Storage cost	High	Medium	Medium	Low	Low
Execution time	High	Medium	Medium	Medium	Low
RSU's overhead	High	High	Medium	Low	Low

In Table 4, we expand the security performance analysis for some more available schemes [43–45] and tabulate the findings. Such an analysis is believed to help future researchers to identify the protocols specific to their area of study. Moreover, it presents a comprehensive survey along with a diversified list of criteria available for further exploration.

Table 4. Summary of performance of various schemes under comparison.

Criteria	[18]	[19]	[20]	[21]	[43]	[44]	[45]	A-MAC
Security against replay attack	✓	✓	✓	✓	✓	✓	✓	✓
Security against impersonation attack	✓	✓	✗	✓	✗	✓	✓	✓
Security against tampering attack	✗	✓	✓	✗	✓	✓	✗	✓

6. Conclusions

A-MAC protocol for secure transmission of data in V2V environment in VANETs is proposed in this article. Along with that, an overview and detailed discussion on five-level architecture to enhance vehicular communication in IoV is presented. The IoV architecture shows great potential in enabling future autonomous driving scenarios. An authentication scheme, A-MAC is proposed. The system necessitates hash operations and upholds the necessary security level. Additionally, the privacy and integrity of the message are protected. We made our system inconsequential by taking less memory and decreasing the number of variables to be stored. The results show that A-MAC protocol outperforms other similar protocols based on hash mechanism. It can withstand common security attacks during data transmission in vehicular scenario.

In future, we look to work on spatial correlation for further analysis of the proposed model. DCF shall be further customized to reduce latency and loss ratio. A hybrid technique that works well with safety as well as security of the data shall be devised. We shall come up with new communication protocols for the IoV framework to resist cyberattacks by verifying security strengths.

Author Contributions: Conceptualization, N.G., R.M. and B.S.; methodology, N.G., R.M. and B.S.; validation, N.G., R.M. and B.S.; writing–original draft preparation, N.G., R.M., B.S. and A.T.; writing—review and editing, N.G., F.S. and A.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors Ariel Teles and Francisco Silva would like to thank FAPEMA (State of Maranhão Research Funding Agency) for supporting their research projects.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADAS	Advanced Driver Assistance System
D2D	Device-To-Device
DAS	Data Acquisition System
DSRC	Dedicated Short-Range Communication
ITS	Intelligent Transportation Systems
IoT	Internet of Things
IoV	Internet of Vehicles
MAC	Media Access Control
MD5	Message-Digest algorithm 5
OBU	On-Board Unit
QoS	Quality of Service
RSU	Roadside Unit
RSA	Rivest–Shamir–Adleman
SSL	Secure Sockets Layer
TA	Trust authority
TCP	Transmission Control Protocol
TLS	Transport Layer Security
V2M	Vehicle-to-Mobile station
V2P	Vehicle-to-Personal devices
V2R	Vehicle-to-Roadside unit
V2S	Vehicle-to-Sensors
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Anything
VANET	Vehicular Ad hoc Network

References

1. Ang, L.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges. *IEEE Access* **2019**, *7*, 6473–6492. doi:10.1109/ACCESS.2018.2887076. [CrossRef]
2. Limbasiya, T.; Das, D. IoVCom: Reliable Comprehensive Communication System for Internet of Vehicles. *IEEE Trans. Dependable Sec. Comput.* **2019**. doi:10.1109/TDSC.2019.2963191. [CrossRef]
3. Gupta, N.; Prakash, A.; Tripathi, R. Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey. *Veh. Commun.* **2015**, *2*, 223–237. doi:10.1016/j.vehcom.2015.10.001. [CrossRef]
4. Kenney, J.B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. doi:10.1109/JPROC.2011.2132790. [CrossRef]
5. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. doi:10.1016/j.jnca.2013.02.036. [CrossRef]
6. Lee, S.; Park, J.; Gerla, M.; Lu, S. Secure Incentives for Commercial Ad Dissemination in Vehicular Networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 2715–2728. doi:10.1109/TVT.2012.2197031. [CrossRef]
7. Yong, X.; Libing, W.; Yubo, Z.; Luyao, Y. Anonymous Mutual Authentication and Key Agreement Protocol in Multi-Server Architecture for VANETs. *J. Comput. Res. Dev.* **2016**, *53*. doi:10.7544/issn1000-1239.2016.20160428. [CrossRef]
8. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1621–1632. doi:10.1109/TITS.2018.2827460. [CrossRef]

9. Cheng, J.; Cheng, J.; Zhou, M.; Liu, F.; Gao, S.; Liu, C. Routing in Internet of Vehicles: A Review. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2339–2352. doi:10.1109/TITS.2015.2423667. [CrossRef]
10. Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1342–1363. doi:10.1109/COMST.2015.2422735. [CrossRef]
11. Zhong, H.; Huang, B.; Cui, J.; Xu, Y.; Liu, L. Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks. *IEEE Access* **2018**, *6*, 2241–2250. doi:10.1109/ACCESS.2017.2782672. [CrossRef]
12. Zhang, C.; Lu, R.; Lin, X.; Ho, P.; Shen, X. An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250. doi:10.1109/INFOCOM.2008.58. [CrossRef]
13. Bazzi, A.; Cecchini, G.; Menarini, M.; Masini, B.M.; Zanella, A. Survey and Perspectives of Vehicular Wi-Fi versus Sidelink Cellular-V2X in the 5G Era. *Future Internet* **2019**, *11*, 122. doi:10.3390/fi11060122. [CrossRef]
14. Cavalcanti, E.R.; de Souza, J.A.R.; Spohn, M.A.; de Morais Gomes, R.C.; da Costa, A.F.B.F. VANETs' Research over the Past Decade: Overview, Credibility, and Trends. *SIGCOMM Comput. Commun. Rev.* **2018**, *48*, 31–39. doi:10.1145/3213232.3213237. [CrossRef]
15. Chen, M.; Tian, Y.; Fortino, G.; Zhang, J.; Humar, I. Cognitive Internet of Vehicles. *Comput. Commun.* **2018**, *120*, 58–70. doi:10.1016/j.comcom.2018.02.006. [CrossRef]
16. Wan, J.; Zhang, D.; Zhao, S.; Yang, L.T.; Lloret, J. Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. *IEEE Commun. Mag.* **2014**, *52*, 106–113. doi:10.1109/MCOM.2014.6871677. [CrossRef]
17. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.; Liu, X. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. *IEEE Access* **2016**, *4*, 5356–5373. doi:10.1109/ACCESS.2016.2603219. [CrossRef]
18. Li, J.; Lu, H.; Guizani, M. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 938–948. doi:10.1109/TPDS.2014.2308215. [CrossRef]
19. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensic Secur.* **2015**, *10*, 2681–2691. [CrossRef]
20. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Trans. Veh. Technol.* **2016**, *65*, 896–911. doi:10.1109/TVT.2015.2402166. [CrossRef]
21. Zhang, L.; Hu, C.; Wu, Q.; Domingo-Ferrer, J.; Qin, B. Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response. *IEEE Trans. Comput.* **2016**, *65*, 2562–2574. doi:10.1109/TC.2015.2485225. [CrossRef]
22. Vijayakumar, P.; Azees, M.; Kannan, A.; Jegatha Deborah, L. Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1015–1028. doi:10.1109/TITS.2015.2492981. [CrossRef]
23. Malik, A.; Pandey, B. Security Analysis of Discrete Event Based Threat Driven Authentication Approach in VANET Using Petri Nets. *Int. J. Netw. Secur.* **2018**, *20*, 601–608. doi:10.6633/IJNS.201807_ 20(4).01. [CrossRef]
24. Ora, P.; Pal, P.R. Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography. In Proceedings of the 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 10–12 September 2015. doi:10.1109/IC4.2015.7375655. [CrossRef]
25. Cao, D.; Yang, B. Design and implementation for MD5-based data integrity checking system. In Proceedings of the 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China, 16–18 April 2010; pp. 608–611. doi:10.1109/ICIME.2010.5477912. [CrossRef]
26. Chawdhury, M.D.A.; Habib, A.H.M.A. Security enhancement of MD5 hashed passwords by using the unused bits of TCP header. In Proceedings of the 2008 11th International Conference on Computer and Information Technology, Khulna, Bangladesh, 24–27 December 2008; pp. 714–717. doi:10.1109/ICCITECHN.2008.4803081. [CrossRef]

27. Liu, J.; Li, Q.; Cao, H.; Sun, R.; Du, X.; Guizani, M. MDBV: Monitoring Data Batch Verification for Survivability of Internet of Vehicles. *IEEE Access* **2018**, *6*, 50974–50983. doi:10.1109/ACCESS.2018.2869543. [CrossRef]
28. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. *China Commun.* **2014**, *11*, 1–15. doi:10.1109/CC.2014.6969789. [CrossRef]
29. Salameh, N.; Challita, G.; Mousset, S.; Bensrhair, A.; Ramaswamy, S. Collaborative positioning and embedded multi-sensors fusion cooperation in advanced driver assistance system. *Transp. Res. Part C Emerg. Technol.* **2013**, *29*, 197–213. doi:10.1016/j.trc.2012.05.004. [CrossRef]
30. Gupta, N.; Prakash, A.; Tripathi, R. Clustering based cognitive MAC protocol for channel allocation to prioritize safety message dissemination in vehicular ad-hoc network. *Veh. Commun.* **2016**, *5*, 44–54. doi:10.1016/j.vehcom.2016.09.004. [CrossRef]
31. Temel, S.; Vuran, M.C.; Faller, R.K. A Primer on Vehicle-to-Barrier Communications: Effects of Roadside Barriers, Encroachment, and Vehicle Braking. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016. doi:10.1109/VTCFall.2016.7880871. [CrossRef]
32. Gao, S.; Lim, A.; Bevly, D. An empirical study of DSRC V2V performance in truck platooning scenarios. *Digit. Commun. Netw.* **2016**, *2*, 233–244. doi:10.1016/j.dcan.2016.10.003. [CrossRef]
33. Xie, Y.; Su, X.; He, Y.; Chen, X.; Cai, G.; Xu, B.; Ye, W. STM32-based vehicle data acquisition system for Internet-of-Vehicles. In Proceedings of the IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), Wuhan, China, 24–26 May 2017; pp. 895–898. doi:10.1109/ICIS.2017.7960119. [CrossRef]
34. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. doi:10.1109/TITS.2017.2657649. [CrossRef]
35. Fortino, G.; Russo, W.; Savaglio, C.; Viroli, M.; Zhou, M. Modeling Opportunistic IoT Services in Open IoT Ecosystems. Available online: http://ceur-ws.org/Vol-1867/w16.pdf (accessed on 26 February 2020).
36. Cugola, G.; Margara, A. Processing Flows of Information: From Data Stream to Complex Event Processing. *ACM Comput. Surv.* **2012**, *44*. doi:10.1145/2187671.2187677. [CrossRef]
37. Tan, H.; Ma, M.; Labiod, H.; Boudguiga, A.; Zhang, J.; Chong, P.H.J. A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9570–9584. doi:10.1109/TVT.2016.2621354. [CrossRef]
38. Vladyko, A.; Khakimov, A.; Muthanna, A.; Ateya, A.A.; Koucheryavy, A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications. *Future Internet* **2019**, *11*, 128. doi:10.3390/fi11060128. [CrossRef]
39. Arena, F.; Pau, G. An Overview of Vehicular Communications. *Future Internet* **2019**, *11*, 27. doi:10.3390/fi11020027. [CrossRef]
40. Libed, J.M.; Sison, A.M.; Medina, R.P. Improved MD5 through the Extension of 1024 Message Input Block. In Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence, Hanoi, Vietnam, 28–30 September 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 18–23. doi:10.1145/3278312.3278318. [CrossRef]
41. Vasudev, H.; Das, D. A Lightweight Authentication Protocol for V2V Communication in VANETs. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation, Guangzhou, China, 8–12 October 2018; pp. 1237–1242. doi:10.1109/SmartWorld.2018.00215. [CrossRef]
42. MathWorks MATLAB. Version 8.5 (R2015a). Available online: https://www.mathworks.com/help/matlab/release-notes-R2015a.html (accessed on 26 February 2020).
43. Ren, C.; Zhang, W.; Qin, L.; Sun, B. Queue Spillover Management in a Connected Vehicle Environment. *Future Internet* **2018**, *10*, 79. doi:10.3390/fi10080079. [CrossRef]

44. Amadeo, M.; Campolo, C.; Molinaro, A.; Harri, J.; Rothenberg, C.E.; Vinel, A. Enhancing the 3GPP V2X Architecture with Information-Centric Networking. *Future Internet* **2019**, *11*, 199. doi:10.3390/fi11090199. [CrossRef]
45. Liu, Q.; Ma, Y.; Alhussein, M.; Zhang, Y.; Peng, L. Green data center with IoT sensing and cloud-assisted smart temperature control system. *Comput. Netw.* **2016**, *101*, 104–112. doi:10.1016/j.comnet.2015.11.024. [CrossRef]