Enhancing Security Communication in Vehicular Cloud through Identifier-Based-Signature Scheme

Hadjer Goumidi
LRSD laboratory, Computer Science Dept
Ferhat Abbas University
Setif 1, Algeria
hadjer.goumidi@univ-setif.dz

Zibouda Aliouat
LRSD laboratory, Computer Science Dept
Ferhat Abbas University
Setif 1, Algeria
zaliouat@univ-setif.dz

Saad Harous
College of Information Technology
United Arab Emirates University
Al-Ain, UAE
harous@uaeu.ac.ae

***Abstract*—The recent improvement in VANET and cloud computing technology has developed the intelligent transportation systems, which raises security problems due to several violations of security policies. It is crucial to prevent vehicles to take in fact forged messages and to preserve the privacy of vehicles. Security and privacy are the major concern in vehicular cloud computing. In this paper, we propose an efficient authentication algorithm using Identifier-Based-Signature (IBS) scheme to provide vehicles' trustworthiness, secure communication and vehicles' privacy. Vehicles' privacy is preserved by using pseudonyms generated by the cloud instead of the real identifiers. V2R and V2V authentication is ensured by using the IBS signature scheme. The performance of our proposed algorithm is compared to recent schemes. Simulation results shows that our proposed algorithm provides secure communication among vehicles with less computation time.**

***Index Terms*—VANET, VCC, Privacy, Authentication, IBS.**

I. INTRODUCTION

The Fast advancement of automobile industry led to development of intelligent transportation systems, which introduced Vehicular ad-hoc network (VANET). VANET is a self-organized network that allows vehicles to communicate with each other with or without roadsides unit (RSU) in order to improve driving safety and traffic management. The Federal communications commission (FCC) of USA has allocated 75 MHz of spectrum for VANET. Dedicated Short Range Communication (DSRC) [4] is reserved for the vehicle communication, and WAVE 802.11p standard to encourage standard communication over the assigned spectrum range by adapting the scarcity of DSRC spectrum for excessive vehicle density. Nowadays, vehicles are equipped with a processing on-board unit, a large capacity storage device, GPS device, cameras, radio transceiver and other types of sensing devices which enable vehicles to collect information about the traffic environment and exchange this information. VANET architecture is integrated with cloud computing to become what is called vehicular cloud computing (VCC) that provides computation and storage capability for this large amount of sensed data.

Recently, many research about security issues have been proposed to provide a secure communication between vehicles, where vehicles' authentication is the most important issue. Hence, authentication provides vehicles' trustworthiness, secure communication and attackers identification to prevent them from injecting, altering and replying messages. Privacy also needs to be preserved to hide vehicles' private information such as driver's name, contact number. etc, from other vehicles in the network. The privacy is generally ensured using a pseudonym instead of the real identifier. Many authentication solutions have been proposed in the literature to ensure vehicles authentication and provide secure communication [7, 2, 5, 6]. Identifier-Based-Signature (IBS) algorithm is used to guarantee entity's authentication, in which it calculates the user's signature from its identity. The verification of the signature requires the knowledge of the signer's identity and the master key. Signature generation is carried out using the following steps: *Setup:* a certified authority generates master key and broadcasts it to all vehicles through RSUs. *Extraction:* Vehicle takes as input its identifier, the master key and timestamp, and outputs its private key. *Signing:* Vehicles will generate signature SIG by encrypting the message M using its private key. *Verification:* Receiving vehicle verifies the signature and accepts it if it is valid, otherwise it is rejected. In this paper, we propose a secure authentication algorithm for VCC members, based on Identifier Based Signature (IBS) to provide a secure communication. We use pseudonym instead of the real vehicles' identifier to provide conductors' privacy. The rest of the paper is organized as fellow:

Section 2 summarizes the existing authentication schemes in the vehicular network, and vehicular cloud. Section 3 explains the proposed system in detail. Section 4 analyses the performance and the simulation results of our scheme. Section 5 concludes this paper.

II. RELATED WORK

In [1] authors proposed an anonymous batch authenticated and key agreement scheme for value added services (ABAKA) in VANETs. This algorithm uses elliptic curve cryptography to provide authentication with less overhead. It provides efficient authentication in a vehicular environment by using one verification operation to authenticate multiple request messages and it uses a detection algorithm in order to deal with invalid request problem. In [3] authors proposed an efficient anonymous batch authentication scheme (ABAH) for vehicular network. This algorithm replaces time consumption CLRs by

978-1-7281-0927-5/19/$31.00 ©2019 IEEE

HMAC. It ensures privacy preservation and batch verification using the pseudonyms and identity-based signature (IBS), respectively. This algorithm guarantees vehicles integrity and secure communication in vehicular environment. Authors in [8] proposed a conditional privacy-preserving authentication scheme (CPAS), where they use a pseudo-identity-based signature to ensure a conditional privacy preserving. This algorithm ensures secure vehicle to RSU communication. It enables RSUs to verify multiple signatures from different vehicles simultaneously, which reduces the total verification time. Authors in [6] proposed a secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing. This protocol ensures the identity privacy of vehicles and their generated messages through pseudonym technique. It uses an anonymous credential technique to generate the authorization of vehicles. ID-Based signature (IBS) is applied to provide vehicle's authentication. Batch verification and pseudonym revocation list are used respectively to make sure the signature and revoked misbehaving vehicles are verified efficiently. This algorithm needs a proper encryption scheme to provide information confidentiality and access authentication which makes it vulnerable. In [7] authors used the IBS algorithm to provide vehicles' authentication, and pseudonym instead of the real identifier to provide vehicles' privacy. This protocol requires that each vehicle must register itself by sending its real ID and its information through a predefined registration process. After verifying its availability and its accessibility, the cloud generates vehicles' pseudonym by encrypting vehicles' ID using the system master key. This scheme uses the CP-ABE algorithm to ensure access control for both VANET and cloud. It signs its messages using IBS signature to ensure V2R authentication. V2V authentication is not considered in this algorithm. The work in [2] proposed an algorithm that uses ID-based signature (IBS) and ID-based online/offline signature (IBOOS) scheme for authentication purpose. The IBS is used to authenticate the communication between vehicles and RSU. IBOOS authenticates the communication between vehicles. the pseudo-ID is used instead of the real ID to ensure vehicles' privacy. Vehicles send their original details during the registration step, the RTA generates vehicles' public and private keys, and then vehicles use their public key to generate their pseudo-ID. In this scheme different types of authentication are carried out. Vehicle to RSU authentication: the RSU affects an offline signature to authenticate vehicles. Inter-vehicles authentication: V2V authentication is carried out using the offline signature generated by the RSU to calculate the online signature. Cross-RSU authentication: vehicles under the control of different RSUs and do not have the offline signature of each other can communicate with each other. Cross-RTA authentication: when vehicles move from one region to another, they must register themselves to another RTA, and then it will calculate its offline/online signature using the same step of inter vehicles and vehicles to RSU authentication. Authentication without RSU: in this case vehicles can communicate securely with one another using RSA algorithm.

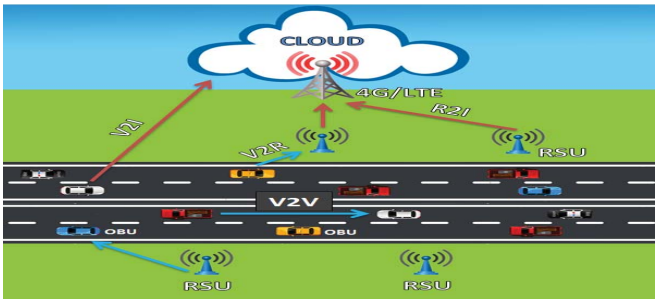

Fig. 1. Network architecture for the proposed approach.

III. Proposed Approach

A. Network Architecture

Our network's architecture is illustrated in Figure 1. It is mainly composed of:

- **Vehicle:** It is the mobile node and the main component for our network architecture. Each vehicle is equipped with on-board wireless device (OBU), GPS (Global Positioning System), EDR (Event Data Recorder) and sensors to sense traffic congestions and status.
- **On-Board Unit (OBU):** It is a device mounted on board in a vehicle to provide a mutual wireless communication between the vehicle and surrounding vehicles and infrastructures. It uses the Wireless Access in Vehicular Environment (WAVE) standard, which is based on the emerging IEEE 802.11p specification [5].
- **Road Side Units (RSU):** These are fixed communication infrastructure units distributed on the roadside for collecting and disseminating traffic-related information. This unit is equipped with at least one network device for the Internet and short-range wireless communication. It acts as a gateway for the OBU to access the Internet, which also enables vehicles within its communication range to Internet access. In the proposed approach, the RSU is the responsible unit for vehicles' authentication by verifying their signature and for authentication key distribution.
- **Vehicle-to-Vehicle (V2V) communication:** It is the basic communication type in VANET. It allows the direct wireless transmission of data between vehicles and does not rely on fixed infrastructure. This type of communication is established if and only if the vehicles are mutually in the communication range of each other. Vehicles need to authenticate themselves before establishing communication between them. Vehicles' authentication is considered as one of the significant challenges in vehicular network security.
- **Vehicle-to-RSU (V2R) communication:** It takes place between vehicles and RSU fixed infrastructure through wireless transmission. In the proposed approach, when a vehicle wants to authenticate itself, it calculates its signature and sends a join raquest to the RSU to get authenticated and to get an authentication key. RSU-to-Vehicle (R2V) communication: It takes place between

TABLE I
VALUE NOTATIONS TABLE

Notation	Value
KGR	Key Generation Request
V_i	Vehicle i
VI_i	Vehicle Information of vehicle i
VID	Vehicle Information Database
PK_i	Public Key of vehicle i
PrK_i	Private Key of vehicle i
$Pseu_i$	Pseudonym of vehicle i
AuK	Authentication Key
SIG_i	IBS signature of vehicle i using its PrK
$AuSIG_i$	IBS Authentication signature of vehicle i using its AuK
D_m	Delay of the transmitted massage
Del	the message delay defined in the RSU
CR	Communication Request
RR	Reception Rate
Msgs	Messages sent
Msgr	Messages received
AuT	Authentication Table
ACC	Table of accepted messages
REJ	Table of rejected messages

RSU and vehicles. In our model, when the RSU verifies the vehicles signature, it sends a reply indicating whether the car is authenticated or not. All vehicles, within the RSU transmission range, receive the RSU's reply message. Once an RSU authenticates a vehicle, vehicles will save the identification of this authenticated vehicle in their authentication table.

- **Vehicle-to-Internet (V2I) communication:** It takes place between vehicles and the internet. It can be established indirectly using the RSU, or directly when vehicles want to access to the cloud for private key generation.
- **Cloud Center:** It is a virtual server that provides several services such as computing capabilities, sensors, storage, and communication resources on demand. In the proposed approach, the cloud is the responsible for keys generation, stores all vehicles' information and it uses this information in vehicle's private key generation.

B. Algorithm Description

In this section, we describe our algorithm construction in detail. Table I presents the different notation used in our scheme. Our proposed algorithm has 4 main steps:

- **Setup:** each vehicle, at the start of its trip sends a KGR to the cloud via a secure channel.

$$\text{KGR} = [ID_i, \text{KEY-R}].$$

The cloud then, extracts the original details of vehicle from its vehicular information database (VID) using its identifier to generate vehicle's private key.
VID: a huge data base, stored in the cloud, contains all private informations of vehicles such as: vehicle identifier, pallet number, vehicles' construction date, vehicles' conductors name.

Setup private key generation algorithm:
Phase1: the cloud inputs vehicle's information (VI_i) and outputs public key (PK_i) of V_i.
Phase2: IBS-KeyGen (PK_i, ID_i). The IBS private key generation algorithm takes the identity of vehicle 'i' and the public key PK_i as input, and outputs the vehicle's private key PrK_i.

- **Pseudonym formation:** after calculating the private key PrK_i of vehicle 'i', the cloud generates vehicle's pseudonym. It encrypts vehicle's identifier using the private key. Then it sends the pseudonym and the private key (PrK_i) to the vehicle 'i'.
- **Registration:** when a vehicle enters in a particular region, it sends a JOIN-Request to the nearby RSU.

$$\text{JOIN-Request} = [Pseu_i, SIG_i, \text{JOIN}].$$

Where SIG_i is the IBS signature of vehicle 'i' calculated by concatenating the ID_i with the current time and encrypting it using the private key PrK_i. We use the current time to ensure the freshness of the JOIN-Request. If an attacker impersonates the identity of V_i it will send its JOIN-Request. The RSU will detect it by verifying the time in SIG_i.

- **Authentication**
V2R authentication: after receiving the JOIN-Request of V_i, the RSU sends the SIG_i to the cloud. The cloud verifies the validity of the identifier. If it is a valid identifier, it sends the ID_i and the PrK_i to the RSU, otherwise it sends a REJECT message as shown in Figure 2.
The RSU then, verifies the time in SIG_i using PrK_i. It calculates message delay (D_m) using formula (1):

$$D_m = T_r - T_e \qquad (1)$$

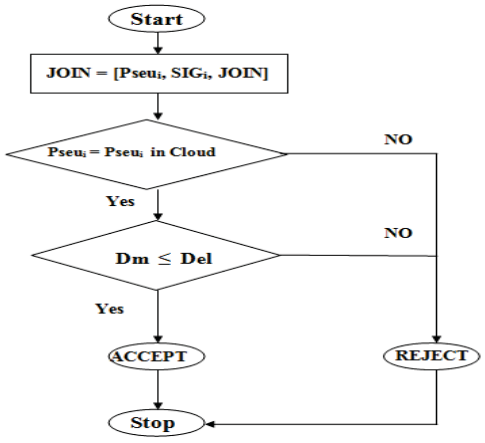

Fig. 2. V2R authentication process.

$$h = Del - D_m, \begin{cases} m \in ACC[i] & , \quad h \geqslant 0 \\ m \notin REJ[i] & , \quad h < 0 \end{cases} \tag{2}$$

It verifies: if D_m exceeds the messages delay defined in the RSU (Del), it will send REJECT, otherwise it will send REPLY, the RSU uses formula (2).

$$\text{REPLY} = [Pseu_i, \text{ ACCEPT, } (AuK)_{PrK_i}].$$

Where, $(AuK)_{PrK_i}$ is the RSU's authentication key given to all authenticated vehicles. The RSU encrypts it using PrK_i and sends it to V_i to prevents malicious vahicles to harm it. All vehicles within RSU's transmission range receive this message, and saves the vehicle's pseudonym in its authentication table.

V2V authentication: When V_i wants to establish a communication with V_j, it will send a communication request (CR).

$$\text{CR} = [Pseu_i, AUSIG_i, \text{JOIN}, ID_{RSU}].$$

V_j searches in its authentication table, if it finds the $pseu_i$, it will verify $AuSIG_i$ using its AuK. If it finds the same Pseudonym encrypted in the signature and saved in the authentication table, it accepts the communication. Otherwise, it sends a REJECT message, as shown in Figure 3.

When a vehicle 'i' wants to communicate with a vehicle V_x which exists in the range of another RSU_x (authenticated by another RSU) it sends a CR message. V_x must send a verification message (VER) to the RSU_x after receiving the CR.

$$\text{VER} = [\ Pseu_x, \text{VER, } Pseu_i, \ ID_{RSU_i}\ ]$$

The RSU_x retransmits the verification message to the other RSU (the RSU that has vehicle i in its transmission range). RSU_i searches for the $Pseu_i$ in its authentication table, if it finds it, RSU_i sends a REPLY-RSU to the RSU_s.

$$\text{REPLY-RSU} = [\ Pseu_i, \text{ ACCEPT, } AuK_i].$$

The RSU_s will retransmit the REPLY-RSU to the vehicle 'x' after encrypting the AuK_i by the PrK_x to keep it secret. V_x then, verifies $AuSIG_i$ using AuK_i, to decide whether accepting communication or not.

Our algorithm detects misbehaving vehicles and isolates them from the network. However, after commuting violations, vehicles detect the attackers (Non-reputation is ensured in our algorithm) and send Revocation Requests to the RSU. The RSU gathers these Revocation Requests to be sure of the attackers, and broadcasts a revocation message to all vehicles within its range. In this manner attackers are detected and revoked from the network.

After the distribution of AuK in a secure manner, we use a symmetric cryptography for V2V and V2R communication. All authenticated vehicles have the AuK, either directly from the same RSU (authenticated by the same RSU) or indirectly from another RSU (authenticated by different RSUs). This is the way, our algorithm ensures a secure communication between vehicles.

Figure 4 shows the sequence diagram of our scheme.

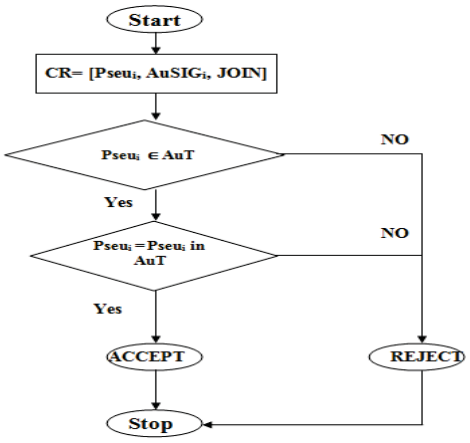

Fig. 3. V2V authentication process.

IV. Performance Evaluation and Security Analysis

In this section, we provide a performance evaluation of the proposed protocol in terms of reception rate, computation delay.

in order to illustrate the efficiency of our proposed scheme, we simulate our algorithm with the parameters illustrated in Table II. We generate this scenario using 'VanetMobiSim' vehicles' mobility generator.

The reception rate (RR) is the ratio of total received packets over total number of transmitted packets from one entity to another.

$$RR = \sum Msg_r / \sum Msg_s \tag{3}$$

The reception rate is computed using formula (3). Figure 5 shows that the reception is improved by about 60% when our scheme is used. This is due to the fact that

TABLE II
Simulation Parameters

Topology (m^2)	2000*2000
Number of nodes	200
Number of RSUs	2
Communication range of nodes (m)	300
Communication range of RSU (m)	1000
Attackers	8 choosed randomly
Speed (m/s)	20
MAC layer	MAC 802_ 11p
Simulation Time(s)	300 s
Mobility model	Random Following IDM_ LC

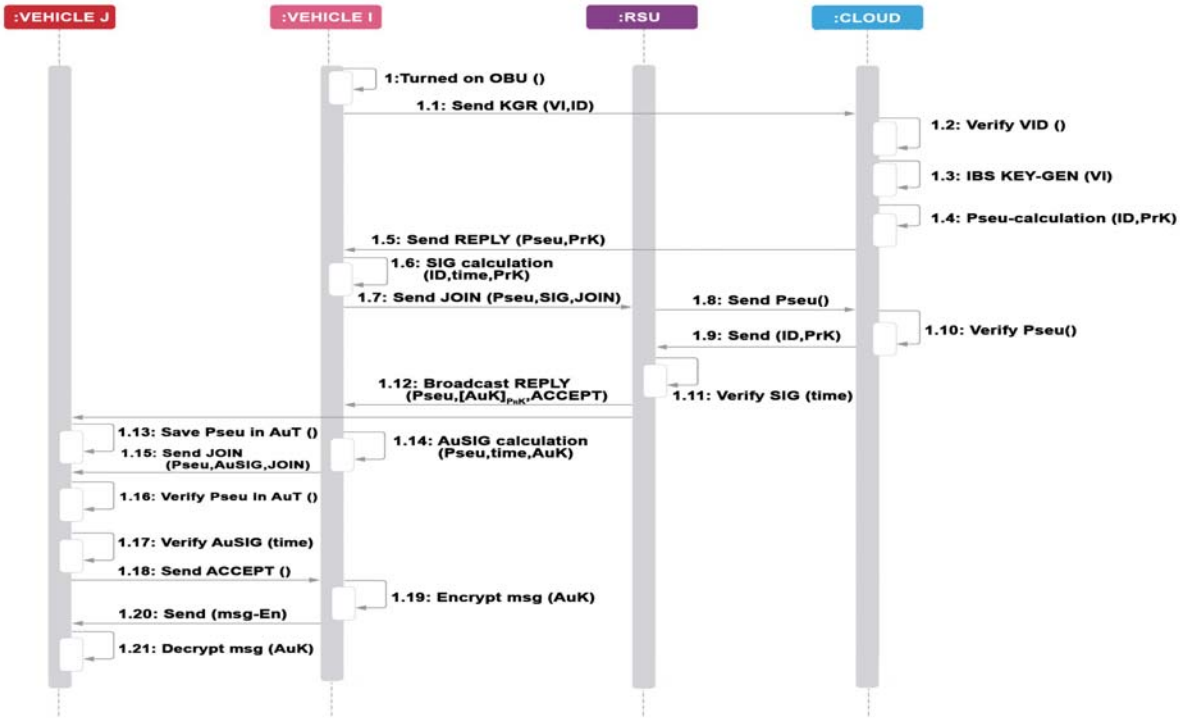

Fig. 4. Sequence diagram of our scheme.

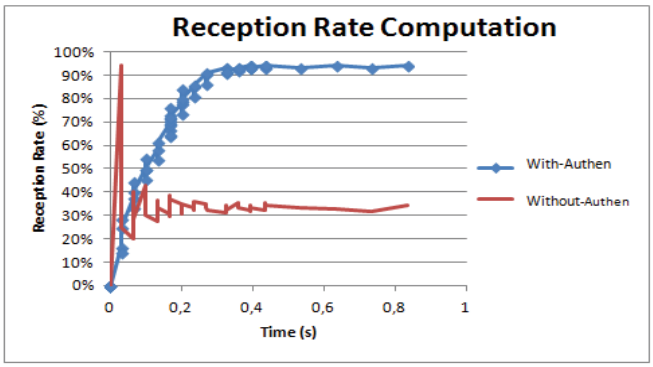

Fig. 5. V2V authentication reception rate.

vehicles are authenticated, so attackers are detected and their messages are not forwarded to other vehicles in the network. But when the vehicles are not authenticated, attackers can inject forged messages and receivers of these messages forward them to other vehicles which saturate the network, that leads to the loss of messages.

Table III presents a comparative evaluation of our algorithm to other scheme [1, 8, 9, 3] in terms of privacy, non-repudiation and computation delay.

Figure 6 represents a comparison of different authentications schemes, in which each OBU has 120 nodes in its transmission range. As shown in Figure 6 our proposed scheme has less transmission delay of 256 (ms) than RAISE, CPAS, ABAKA, ABAH and IBS/IBOOS which respectively and approximately have 1100 (ms), 800 (ms), 790 (ms), 770 (ms) and 370 (ms).This difference in the delay transmission is due to the computation time of the cryptography method and the algorithm proposed in the scheme. RAISE algorithm uses the MAC cryptography. ABAKA uses the Elliptic curve cryptography. CPAS uses IBS scheme, but the algorithm used to ensure authentication requires height computation and verification time. ABAH uses both HMAC and IBS signature, it has almost the same transmission delay with ABAKA and CPAS. However, IBS/IBOOS algorithm has a lower transmission delay compared with the previous because of the algorithm used, it uses IBS signature for V2R authentication and IBOOS for V2V authentication. In our scheme we also use IBS signature, for V2V and V2R authentication, but we have the lowest transmission delay this is due to the algorithm proposed.

As presented, IBS/IBOOS has the nearest transmission delay to our algorithm. In order to be more precise we compared our algorithm signature calculation with that of IBS/IBOOS as shown in Figure 7. IBS/IBOOS generates four signatures to ensure its V2V and V2R authentication. It took 442 μs to generate its authentication, in which the RSU generates the signature SIG_R in 72 μs, the signature generated by vehicle z (SIG_z) took 142 μs, 127 μs for the offline signature generated by vehicle z ($SIG_z^{offline}$)and the online signature generated by

TABLE III
COMPARISON WITH OTHER AUTHENTICATIO SCHEMS

Schemes	Cryptography basis	privacy	Computation Time	Non-Repudiation
ABAKA [1]	Elliptic curve cryptography	No	Medium	No
CPAS [8]	Identity based signature	No	Medium	No
RAISE [9]	MAC	Yes	Hight	No
ABAH [3]	HMAC and IBS	Yes	Medium	No
IBS/IBOOS [2]	IBS and IBOOS	Yes	Low	Yes
Our	IBS	Yes	Low	Yes

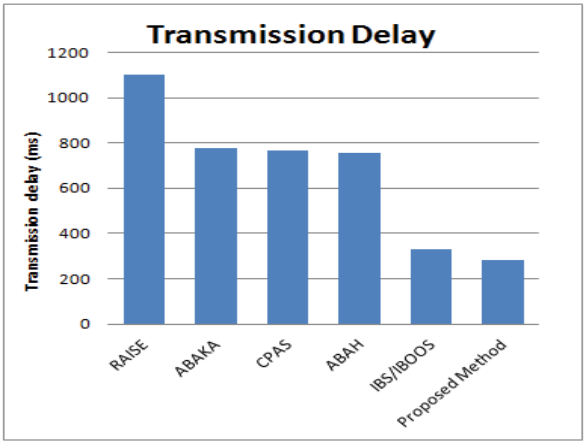

Fig. 6. Comparing average transmission delay of the existing schemes.

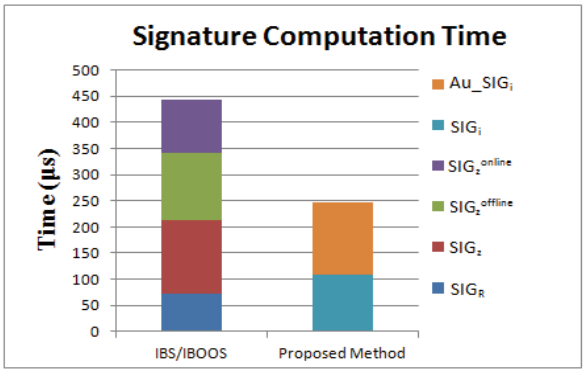

Fig. 7. Comparing signatures computation time of IBS/IBOOS and our protocol.

vehicle z (SIG_z^{online}) took 101 μs.

Meanwhile, our algorithm generates two signatures to ensures V2R and V2V authentication, it takes only 242 μs to generate its authentication as shown in table IV, the signature generated by vehicle 'i' (SIG_i) to send JOIN message to the RSU has a delay of 109 μs, The delay of authentication signature generated by vehicle 'i' $AuSIG_i$ to send JOIN message to vehicle 'j' is 138 μs.

TABLE IV
SIGNATURE COMPUTATION TIME

Signature generation	Computation time (μs)
SIG_i	109
$AuSIG_i$	138

V. CONCLUSION

In this paper, we propose an efficient authentication scheme using IBS signature for vehicular cloud computing. Our proposed algorithm ensures vehicles authentication. It secures communication using 'AuK' generated by the RSU for all authenticated nodes. Also, vehicles privacy using pseudonym generated by the cloud instead of the real identifier. Simulation results show that our algorithm improves the reception rate and computation delay. Our algorithm detects the attackers, rejects their communication and prevents them from harming the messages transmission. We compare our protocol to the existing authentication schemes in term of computation delay.

VI. ACKNOWLEDGMENT

This research work is supported in part by PHC-Tassili Grant Number 18MDU114.

REFERENCES

[1] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "Abaka: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

[2] J. Jenefa and E. M. Anita, "Secure vehicular communication using id based signature scheme," *Wireless Personal Communications*, vol. 98, no. 1, pp. 1383–1411, 2018.

[3] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on hmac for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[4] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[5] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, p. 745303, 2015.

[6] L. Nkenyereye, Y. Park, and K.-H. Rhee, "Secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing," *The Journal of Supercomputing*, vol. 74, no. 3, pp. 1024–1044, 2018.

[7] Q. G. K. Safi, S. Luo, C. Wei, L. Pan, and G. Yan, "Cloud-based security and privacy-aware information dissemination over ubiquitous vanets," *Computer standards & interfaces*, vol. 56, pp. 107–115, 2018.

[8] K.-A. Shim, "backslash*calcpas*: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[9] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.