Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 3, March 2021, pp. 1808~1819
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i3.pp1808-1819

Towards design strong emergency and COVID-19 authentication scheme in VANET

Akeel Kassim Leaby[1], Ali Yassin[2], Mushtaq Hasson[3], Abdullah Rashid[4]
[1,2,3]Computer Science Department, Education College for Pure Science, University of Basrah, Basrah 61004, Iraq
[4]Education College for Human Science, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Aug 21, 2020
Revised Dec 2, 2020
Accepted Dec 22, 2021

Keywords:

Authentication
COVID-19
ECC
Emergency vehicles
Insider attacks
VANET

ABSTRACT

The wide use of vehicular ad hoc networks (VANETs) in the last decade has led many researchers to find efficient and reliable methods to obtain the desired benefits and offer services, such as healthcare and traffic management. However, VANETs suffer from security issues represented by authentication and data integrity. In this paper, we propose a robust mutual authentication scheme based on elliptic curve cryptography (ECC), cryptography Hash Function, and a pseudonym. The proposed work was twofold in focus: first, on healthcare in emergency cars which use VANETs, and second, on overcoming security issues, such as resisting familiar attacks (e.g. insider attacks and reply attacks). Because of the serious situation generated by the worldwide outbreak of the Covid-19 epidemic, we also found this research valuable in supporting global efforts to combat the rapid spread of this virus, by finding the safest and fastest routes to epidemic treatment centres for medical staff, assistance teams in medical operations, fumigation control, and all work teams associated with disease control. This research attempts to contribute by proposing a special signal used to define epidemic teams. The best route, fast route can be chosen by using VANETs infrastructure. This scheme also deals with metric security features, such as key management, data integrity, and data privacy. In the communication and computation cost, we noticed that our proposed scheme achieved good results compared with the related works.

Corresponding Author:

Akeel Kassim Leaby
Computer Science Department
Education College for Pure Science
University of Basrah, Basrah 61004, Iraq
Email: akeel.kasim@uobasrah.edu.iq

1. INTRODUCTION

The rapid growth of wireless networking technology led to the creation of a special type of wireless communication called the internet of vehicles (IoV). The most popular form of the IoV is the VANET. It has been widely used on the roads to achieve several goals: flow and congestion control [1], accident avoidance, improving the safety of motor vehicles, and knowledge of the real-time location of vehicles. In fact, drivers can obtain information about the situation of their route in terms of weather and traffic, the vehicles surrounding them, and how to avoid road problems [2]. Every vehicle can connect to the nearest vehicle through open-source media based on road side units (RSUs), which are considered the main VANET component. VANETs are generated by applying the principles of mobile ad hoc networks (MANETs). These types of networks were introduced in 2001 under vehicle-to-vehicle (V2V) communication and networking applications, where the networks can be created and beacons relayed among vehicles. V2V and vehicle-to-

roadside communications (V2I) architectures will co-exist in VANETs to provide navigation, road safety, and other services. VANETs are a part of the intelligent transportation system (ITS) framework, sometimes referred to as the intelligent transportation network (ITN) [3]. Figure 1 explains the main three entities of VANET as follows: on-board unit (OBU) which carries the same name of the vehicle, road side unit (RSU), and trusted authority server (TAS). Each component carries out specific tasks such as producing system limits, identifying trespassers and registering vehicles that TAS relates. RSUs are nodes that are deployed en route and act as a relay for vehicles, exchanging beacons among vehicles (OBUs) inside the range of RSUs known as V2V. The interchange of beacons between the vehicles (OBUs) and the VANET infrastructure (RSUs) is referred to as vehicle-to-infrastructure (V2I) communication.

VANET uses IEEE 802.11p protocol in V2V and V2I communications. IEEE 802.11P is the basis of dedicated short-range communications (DSRC) and is an approved change to the IEEE 802.11 standard. The newer version has wireless access in vehicular environments (WAVE); it defines enhancements to 802.11 (the basics of products marketed as Wi-Fi) to support intelligent transportation systems (ITS) applications. Information between high-speed vehicles and VANET infrastructure is exchanged using a 5.9 GHz (5.85–5.925 GHz) band. IEEE 1609 is a higher-layer standard based on IEEE 802.11p; it is also the basis of a VANET uses IEEE 802.11p protocol in V2V and V2I communications. IEEE 802.11P is the basis of dedicated short-range communications (DSRC) and is an approved change to the IEEE 802.11 standard. The newer version has wireless access in vehicular environments (WAVE); it defines enhancements to 802.11 (the basics of products marketed as Wi-Fi) to support intelligent transportation systems (ITS) applications. Information between high-speed vehicles and VANET infrastructure is exchanged using a 5.9 GHz (5.85–5.925 GHz) band. IEEE 1609 is a higher-layer standard based on IEEE 802.11p; it is also the basis of a European standard for vehicular communication known as ETSI ITS-G5. Indeed, all of the messages in VANET are exchanged via open-source media [4]. This study proposes an authentication scheme for the VANET environment that uses elliptic-curve cryptography (ECC), a cryptography hash function (SAH-512), to prepare the pseudonyms and other encrypted information for each vehicle. Our work has several benefits, such as mutual authentication, a secure management key, user identity recognition, resistance to well-known attacks (e.g., reply, man in the middle [MITM], and insider attacks), and preserving VANET data privacy. The proposed scheme supports the health care domain in terms of emergency vehicles, especially for ambulances and COVID-19 virus treatment teams. The scheme can provide these vehicles with the shortest route and suggest alternative routes if any congestion or accidents occur based on its knowledge of COVID-19 treatment centre locations.

The rest of the paper is organised as follows: Section 2 demonstrates the primitives and system model, Section 3 explains the related works, Section 4 provides a detailed outline of the proposed scheme, Section 5 contains a security analysis and reports on the experimental results and Section 6 concludes.

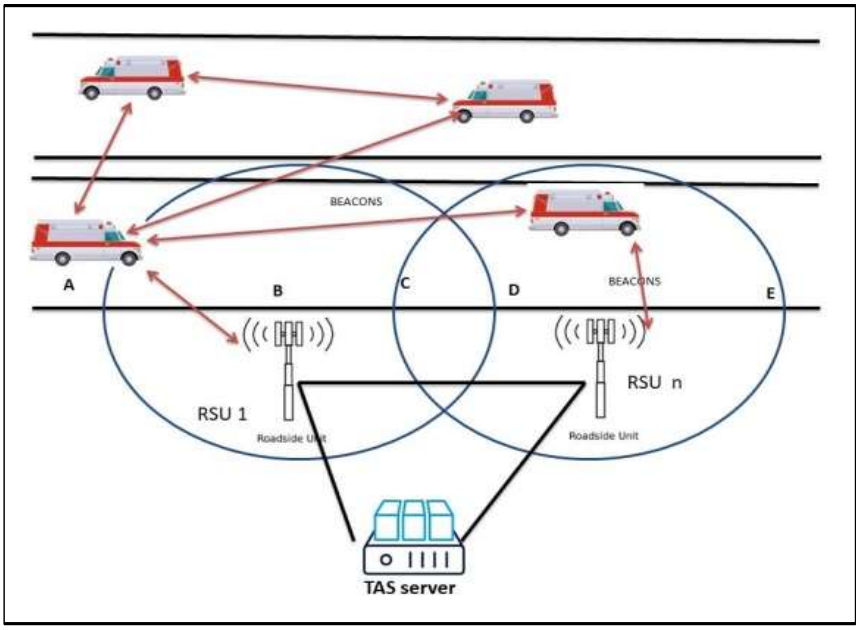

Figure 1. VANET components

2. PRIMITIVES AND SYSTEM MODEL

This section describes all of the proposed scheme requirements to achieve the main goals. It beings by explaining the physical components necessary for a VANET environment. It then demonstrates a VANET's security and privacy requirements and the mathematical tools used in this work.

2.1. Cryptographic TOOLS

a) Elliptic curve cryptography (ECC)

This type of cryptographic tool has become widely used to design security methods and digital signatures. It first appeared in 1958, designed by Miller [1].

b) SHA-512 cryptographic hash function algorithm

Secured Hash Function 512 is a part of the U.S Federal Information Processing Standard and one of a set of hash functions designed by the national security agency (NSA) in the United States of America [5-8].

2.2. System model

The proposed scheme contains the following components:

c) Trusted authority server part (TAS) has the following features: Fully trusted and possesses locations of all components, generates system parameters and processes the joining requests, connected with RSUs via secure wired system and communicates with RSUs in real time procedures and can generate any message if needed.

d) RSUs with the following specifications: deployed overall road to construct VANET range, the neighboured RSUs have a small conferenced area to keep OBUs connected to the system, Route and interchange information between vehicles and infrastructure, and RSUs are connected to each other and to TAS via secure wired systems to keep security and integrity.

e) Vehicle's onboard unit (OBUs) has the following specifications: Use IEEE 802.11p protocol to manage transmission of data with each vehicle and infrastructure, has temper proof device (TPD), accountable for implementing cryptography and security parameters and Has 100s of meters of transmission range.

2.3. Main issues

VANET is a self-organised network. So, emergency vehicles and COVID-19 teams who use this system will face many problems. We can summarise them as follows: *Information security* [9], **Performance, Health care, COVID-19 pandemic, and Quality of Service (QoS).**

3. RELATED WORKS

In recent years, many authors have focused on VANET security and privacy issues. Some of these works can be illustrated under two main categories: public key infrastructure (PKI) and identity-based (ID) schemes.

In PKI-based schemes, the real identity of vehicles is hidden using covered certification. In these schemes, a vehicle obtains a number of certificates during the registration phase using its private key- pairs. Raya and Hubaux [5] proposed a PKI-based scheme. Certificate authority (CA) is responsible for generating private and public keys, as well as certification. These parameters, represented as large numbers, are used to sign and encrypt all the vehicle's messages. This procedure ensures message integrity, but it is restricted by the storage size of the on-board unit (OBU) which is limited and cannot store a large number of private/public keys. Another problem is the time delay caused by a large certificate revocation list (CRL). In 2008, Lu et al. [6] proposed ECPP in relation to security in VANET. ECPP tries to solve the storage space limitation and the increase in CRL by completing the pseudonym computation inside RSUs. Zhang et al. [7] proposed a scheme based on k-anonymity and using a hash authentication message. They named their new scheme RAISE, which stands for efficient roadside aided. In this scheme RSUs are responsible for giving verifications, this leads to minimize the computation cost and ensure vehicle privacy. Rajaput et al. [8] introduce HPPPA which is suggested to solve PKI drawbacks.

In HPPPA, CRL management is not required and only two pseudonyms obtained for each vehicle, based on its key pairs. This protocol faces a problem with the storage of certifications and the management of keys. In 2018, yang et al. [9] proposed CCPPA PKI- based protocol. This work satisfied requirements of security and privacy in VANET and do not employ map-to-point hash function to achieve the best message verification. **ID-based schemes** were proposed to disentangle the problem of emerging in PKI-based schemes. Zhang et al. [10] they use id-based aggregate signature and bilinear cryptography to propose conditional privacy-preserving protocol. This approach uses hierarchy in gathering signatures and patch verification. Although this technique reduces transmission cost and storage exploitation, but it also reduces waiting time for aggregation. Zhang et al. [11] Assumes RSUs as trusted party in VANET. Then, multiple

trusted authorities occur inside VANETs body. Authentication in this paper depends on ID-based signature aggregation. In this work, the distribution of certificates is not centralized and computation is overhead. C. Zhang et al. [12] Proposed IBV scheme. In any time windows, the verification of the received signatures are allowed by batch verification and it is more efficient and faster than if done using single step\single signature verification. Although this scheme can satisfy the above goals, it cannot satisfy the security issues and it is weak toward DOS attacks. Lee and Lai [13] try to improve ID scheme to give an advance in security issues related to scheme that proposed by c.zhang et al. [12]. The new scheme adds pseudonym ID-based generation, message verification, and message signing techniques. However, when the number of valid signature increases, we note degradation in performance. Vijayakumar et al. [14] in 2016 adopted ID-based scheme to propose dual authentication and key management for secure data transmission in VANET. In this research TA can divide vehicles to primary and secondary groups and each group has its specific keys. The reference of vehicles classification is according to the service level agreement SLA, that's means TA will provide two types of services. The entire shared group keys refreshed when any user joins or leaves VANET. It is important to note that although this technique offers forward/backward security, the privacy issues are not addressed. Wang and Nianmin [15] proposed LIAP in 2017. This scheme deals with VANETs ID-based problems such as complicated revocation and holds too many valid identities to protect vehicle privacy. Vehicles and RSUs are given long term authentication. Although this scheme can meet the security and privacy requirements but neglects the redundant authentication overhead. In 2020, Ali et al. [16] proposed IBS-CPPA. This scheme is based on ECC and hash function encryption in V2V broadcasting and support batch signature models to enable vehicles to authenticate a large number of beacons at the same time. IBS-CPPA focuses only on V2V communication but it neglects V2I broadcasting which affects in some way both system performance and V2V broadcasts load and cost computation. Table 1 explains a comparison between our work and other related work in some features.

Table 1. Comparison between proposed scheme and related works

Feature	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]	[21]	Our work
Covid-19 virus solutions	No	No	No	No	No	No	No	No	No	No	No	No	Yes
Health care solutions	No	No	No	No	No	No	No	No	No	No	No	No	Yes
meet the revocation requirement	No	No	No	No	---	No	No	No	No	No	No	---	Yes
Resist insider attacks	Yes	Yes	No	No	---	Yes	Yes	No	Yes	Yes	Yes	---	Yes
Central verification	Yes	Yes	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Central authority center	Yes	Yes	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Designed for any size of VANET system	No	No	Yes	No	No	No	No	Yes	Yes	Yes	No	---	Yes
Meet security requirements	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Meet privacy requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process and storage problems	Yes	Yes	Yes	No	No	No	Yes	No	No	Yes	Yes	---	No

4. PROPOSED SCHEME

The proposed scheme constructed from six different phases. These phases form two different procedures based on special flag (SF) value. This flag involved in joining request message. SF value decides the type of vehicle either normal if (0) or emergency if (1). The rest of this section describes all phases and where use. As shown below, Figure 2 describes normal vehicles procedures, and Figure 3 for emergency and COVID-19 vehicles procedures. To ease the understand all equations, Table 2 shows all notations we used in our proposed scheme. Initialization phase: used in both SF values. This phase deals with system parameters initialization and broadcasting to all RSUs and OBUs. This phase operation is the responsibility of TAS. The registration phase is the second phase. This phase related with vehicle registration. Although registration phase is applied for both SF values, the result is two different types of pseudonyms. When vehicle sends joining request to system by send its public key, password, and SF value to the nearest RSU. Then it will get a pseudonym that is used to hide vehicle real identity. The pseudonym resulted from this phase depends on (SF) value. Third phase is Joining phase. In this phase, the legal vehicles signature and other parameters that permit to beacons broadcasting and verifying operations will calculated. The signature also depends the value of SF flag. When SF=1, permission given to broadcast for both RSUs and OBUs, while when SF=1, broadcasting is allowed only for RSUs. The broadcasting phase begins when vehicles broadcast beacons. Beacons contain different types of information. As illustrated in joining phase, SF value control the type of broadcasting. Renewing signature phase. When vehicles owned its signature, this signature has life-time. This life-time always checked if expired and renewed if the vehicle is valid. The important note that emergency vehicles excluded from renewing signature operation to improve performance and increase

privacy and security issues for all emergency vehicles. In parallel with previous phases, vehicles will trace and revoke if necessary in **Trace and revoke** phase. Any malicious vehicles appears aggressive against system or penetrated will trace. The action against these hostilities vehicles is to expel it and prevent from renewing signature. The trace and revoke operations includes both normal and emergency vehicles. As we described in the previous section these phases can be explained in details as follows:

4.1. Initialization phases

TAS initiates and broadcast all system parameters using secured channel. In this phase, TAS always updates system parameter to maintain system security. Initialization and broadcasting system parameters can describe in the following steps:-TAS select pairs of large primary numbers p,q . An additive group **A**, which includes all Elliptic Curve **EC**, where EC defined by equation: - $\boldsymbol{g^2 = x^2 + ax + bmodep}$. Where $\boldsymbol{a, b} \in \boldsymbol{Fp}$ **.**

a) TAS generates random number $\mathbf{r}, \boldsymbol{r} \in \boldsymbol{Zq}$ as private key. Then calculate the public key $\boldsymbol{pubk = r.p}$.
b) **TAS** generates three hash functions $h1 = A \rightarrow Zq$,$h2{:}\{0,1\} \times \{0,1\} \times A \times Zq$,$h3{:}\{0,1\} - Zq$. These three hash functions represent cryptographic hash functions.
c) TAS loaded the private key to all RSUs in system.
d) The final step is broadcasting $(q, pubk, p, h1, h2, h3)$ parameters to all RSUs via secured channel (wired channel).

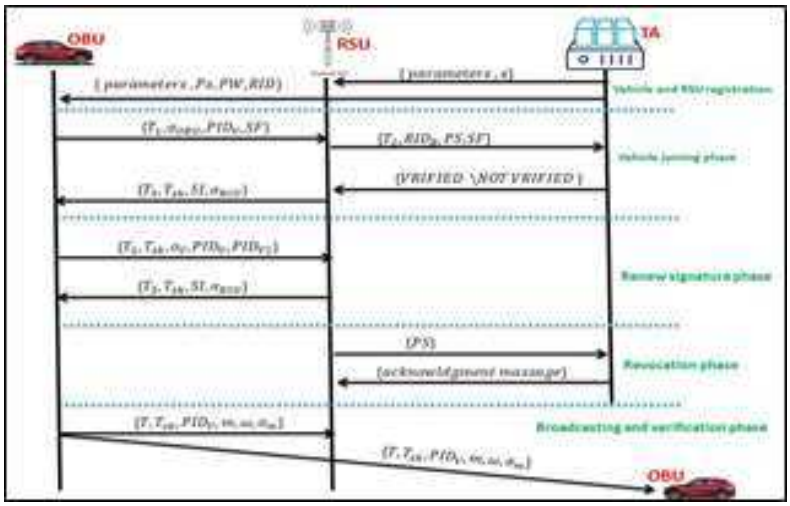

Figure 2. Normal vehicles operation scheme

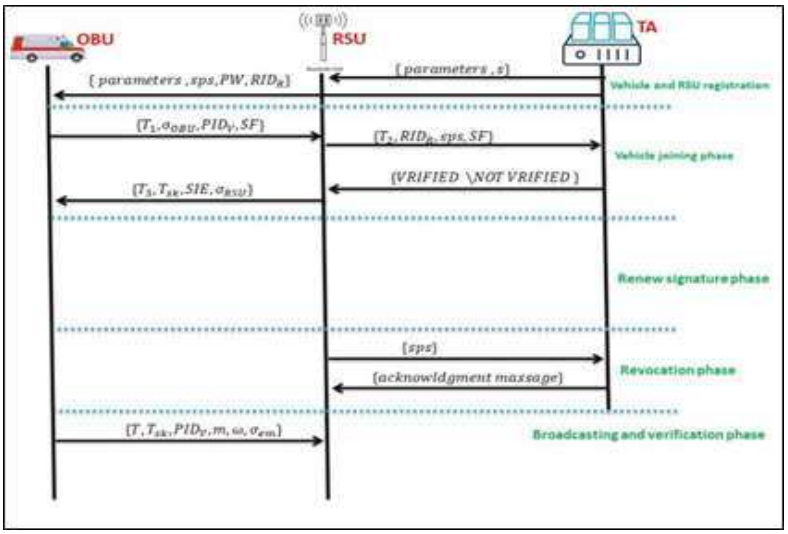

Figure 3. Emergency vehicles operation in the proposed scheme

Table 2. Notations and their descriptions

Notation	Description	Notation	Description
EC	An elliptic curve	$\|$	Concatenation operator
A	An additive group based on EC	$\oplus$	Exclusive OR (XOR) operation
P	A generator of A	SI	The signature of the beacon issued from the RSU
p, q	Large prime numbers	m	Traffic-related message
s, Pubk	Private and public key pairs	T_{sk}	The timestamp of the signature
$h1, h2, h3$	Three secure hash functions	$T_{s1,}$ T_{s2}, $\triangle T$	Timestamp, receiving time and time delay values
RID_R, RID_V	Real identities of the RSU and vehicle	Abbr	Abbreviation of cryptography operations
PID_{v1}, PID_{v2}	Pseudonyms of the vehicle for broadcasting	MBVO	Multi Beacons Verification Operations.
Ps	Pseudonym of the normal vehicle to hide its real identity	SBVO	Single Beacon Verification Operations
SPS	Pseudonym of the emergency vehicle to hide its real identity	BGS	Beacons Generation and Signing
r	Random integer	PW	Password

4.2. Registration phase

The registration for any new user need to join VANET passes through number of steps to approve legality. These steps sequnsly (the user sends join requests message, including vehicle's real identity RID_v and password (pw) across a secured channel to keep privacy and security of the user and system. The join request message contains special flag SF. It either contains 0 if a normal vehicle needs to join or if an emergency vehicle needs to join. And if SF=0 then (TAS checks the validity of(RID_v), Calculate the pseudo name for normal vehicles $\boldsymbol{ps = h3(RID_v \| r)}$**, and** TAS sends $(\boldsymbol{ps, pw}, RID_R)$ to all RSUs and carTPD). While when SF=1, the procedure of registration will be (TAS checks the validity of(RID_v), TAS calculates the pseudo name of emergency vehicle $\boldsymbol{sps = h3(RID_v \| r)}$**, and** TAS sends($\boldsymbol{sps}$**, pw,** RID_R) to all RSUs and carTPD.).

4.3. Joining phase

By creating mutual authentication for every vehicle, the joining phase can summarized as follows: Inside vehicles OBU, (r) will generated where r$\in Z_q$. And OBU will calculate the value of (PID_{V1}, PID_{V2}) which represent the pseudonym of the vehicle. This pseudonym is used to hide the real identity of vehicles. These parameters are calculated as follows: $PID_{V1} = r.P$, $PID_{V2} = ps \oplus h1(r.pubk)$,σOBU= $h3(T_{s1} \| ps)$ $if\ SF = 0$, $PID_{V1} = r.P$, $PID_{V2} = sps \oplus h1(r.pubk)$,σOBU= $h3(T_{s1} \| sps)$ $if\ SF = 1$, When OBU completes the estimation of PID_{v1}, PID_{v2}, it will send the parameters $(PID_{V1}, PID_{V2}$, σOBU) to the nearest RSU. When RSU receives the parameter massage from OBU, the next steps will Check the validity of ($T_{s1)}$ by supposing (T_{sr}) which represents the receive time and if $(T_{sr} - T > \triangle T)$ it will reject the massage because of no validity occurred. Otherwise, it calculates $ps = PID_{v2} \oplus h1(s.PID_{v1}), OR\ sps = PID_{v2} \oplus h1(s.PID_{v1})$ Check if the equations $\sigma OBU = ? h3(T_1 \| ps)$ $or\ the\ equation\ \sigma OBU = ? h3(T_1 \| sps)$ is true. If false, RSU will reject the massage. However, RSU will send the parameters $((T_{s2}, RID_R, sp)$ $if\ SF = 0$, $(T_{s2}, RID_R, sps) if\ SF = 1)$ to TAS.

When TAS receives the parameters $(T_{s2}, RID_R, sp \backslash sps)$ from OBU, then TAS will first check the validity of timestamp (T_{s2}). If valid, TAS's next step is to check the match between the stored $(RID_R, sp \backslash sps)$ and the received one. If matched, the message (verified) will be sent to RSU. If any of the above conditions $((T_{s2})$ $not\ valid\ or$ $(RID_R, sp \backslash sps)$ is not matched, then the message will reject and "not-verified" will be sent to RSU. The content of the massage received by RSU will control the following action from RSU. It will be one of the following procedures. If the message is verified, RSU will complete the signature$(SI) for\ normal\ vehicles\ or (SIE) for\ emergency\ vehicles$. Also it calculates the validation time for normal vehicles only as (T_{sk}). These signatures will be calculated by the following equations if $SIE = s.h2(PID_{v1} \| PID_{v2} \| T_{sk})$ $for\ SF = 1$ or $SI = s.h2(PID_{v1} \| PID_{v2} \| T_{sk})$ $for\ SF = 0$

In the last step of the (verified) message, RSU will send a continue message containing the following parameters $(T_{sk}, T_{s3}, SI_{enc}, \sigma RSU)$ to normal vehicles OBUs or (SIE_{enc}, $T_{s3}, \sigma RSU)$ to emergency vehicles OBUs. Where$(\sigma RSU = h2(SI \| T_{s3} \| T_{sk}), SI_{enc} = SI \oplus h1(s.PID_{v1}), SIE_{enc} = SIE \oplus h1(s.PID_{v1})$

If the massage content is (not verified), RSU will reject the massage and the vehicle will be identified as illegal car. When the parameters $(T_{sk}, T_{s3}, SI_{enc}, \sigma RSU)$ are received by normal vehicles OBUs, or ($SIE_{enc}, T_{s3}, \sigma RSU)$ by emergency vehicles OBUs, they will first check the validity of(T_{s3}). If valid, OBU will compute $(SI\ or\ SIE)$ by using the following equations: $(SI = SI_{enc} \oplus h1(r.pubk)$, $SIE = SIE_{enc} \oplus h1(r.pubk)$, $\sigma RSU = ? h2(SI \| T_{s3} \| T_{sk}))$.

The OBUs of these cars that possess (SF=0) will begin broadcasting its (SI) to the nearest OBUs by sending beacons. While for emergency vehicles, there is no need to transmit beacons to other OBUs. Only Broadcast beacons continue their signature (SIE) for the nearest RSUs according to our proposed scheme.

These beacons contain in addition to signatures many of parameters such as (direction, speed, location, velocity and health care information for ambulance cars).

4.4. Renew signature phase

This phase is applied only for normal cars whose value of the status flag is (SF=0). The renewing signature phase must be applied to renew the expired signature (when $T_{sk}\ expired$). The OBU will renew the signature with the nearest RSU without the need to transmit or receive any information with TAS. This operation is completed by applying the following steps: OBU will generate random integer(r^{new}), where($r^{new} \in z_q$). Then will calculate (PID_{vn}) where :-$PID_{vn1} = r^{new}.p$, $PID_{vn2} = Ps \oplus h1(r^{new}.pubk)$

OBU sends a message containing parameters ($T_{sk}, T_{s1}, PID_{vn1}, PID_{vn2}, \sigma v$) to RSU. Where $\sigma v = SI + r.h2(\ T_{s1} \parallel\ PID_{vn1} \parallel\ PID_{vn2})$. When RSU receive these parameters ($T_{sk}, T_{s1}, PID_{vn1}, PID_{vn2}, \sigma v$), it check the validity of (T_{s1}). If not valid, RSU will reject the massage and new joining phase must be implemented by OBU. While if (T_{s1}) is valid, then the next step is to check the validity of (T_{sk}) by calculating the time required to request new signature(SI). But if (T_{s1}) not valid and request new signature it first check the validity of the vehicle using the following (1):

$$\sigma_v P = h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk}).pubk + h2(PID_{vn1} \parallel PID_{vn2} \parallel T_{s1})PID_{v1} \quad (1)$$

If the result shows that this car is not valid, it will reject the massage from RSU. While valid cars will complete its new signature (SI^{new}) with RSU where:- $SI^{new} = s.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_{sk})$

(T_{sk}) is the new expiration time for new signature. When the new signature is ready to use, RSU will send the following parameters to OBU. ($T_{s2}, T_{sk}, SI_{enc}, \sigma RSU$) Where: $SI_{enc} = SI^{new} \oplus h1(s.PID_{vn1})$, , $\sigma RSU = h2(SI^{new} \parallel T_{s2} \parallel T_{sk})$. When OBU receive the massage from RSU, it will first check the validity of time stamp(T_{s2}). If this parameter is valid, OBU will calculate $SI^{new} = SI_{enc} \oplus h1(r^{new}.pubk)$, the next step is to calculate if the following equation is true: $\sigma RSU = ? h2(SI^{new} \parallel T_{s2} \parallel T_{sk})$. If this equation is equal, the new signature SI_{new} will be valid and can be used with all RSUs. The car when moving inside VANET will receive a valid signature without announcing TAS. For emergency cars, this procedure will be dedicated by sending the signature (SIE) which is calculated previously in the joining phase to all RSUs only and no beacons will be distributed with other cars. If any malicious action or broadcast bogus beacons are sent to any car or RSU, this vehicle will be traced and revoked by informing all RSUs to delete its signature and do not deal with it.

4.5. Broadcast and verification phase

These cars that possess value of SF=0 will finally broadcast beacons for both RSUs via V2I massages and another OBUs via V2V massages. In our proposed scheme, only normal vehicles can do this. The emergency cars which the system can differentiate by their SF value which equals 1, cannot broadcast to other OBUs. They only send beacons to RSUs with their special signature (SIE). So, this section will discuss how these broadcasting operations go ahead. After OBU joins RSU, it will start broadcasting using its signature ($SI\ or\ SIE$) as follows: OBU calculate the massage signature $\sigma m = SI + r.h3(m \parallel T)\ for\ normal\ cars, \sigma em = SIE + r.h3(m \parallel T)\ for\ emegency\ cars$.

OBU computes verification time for receptor(ω) only for normal cars. $\omega = h3(m \parallel T)PID_{v1}$OBU for normal vehicles broadcast the following parameters ($T, T_{sk}, m, \omega, \sigma m, PID_{v1}$) for both RSUs and OBUs. While the situation in emergency vehicles broadcast for RSUs only by sending beacons continue ($T, T_{sk}, m, \omega, \sigma em, PID_{v1}$) and information.

4.6. Vehicle revocation phase

This is an important phase because it allows TAS to trace vehicles against any malicious authentication or any bogus broadcasting. TAS is not only able to trace but also can revoke these vehicles with the end of(T_{sk}). Trace and revoke procedures can be summarized the following steps:

If any vehicle broadcast bogus beacons, RSU computes its pseudonym $(ps)\ for\ normal\ vehicles\ , (sps)\ for\ emegency\ cars.$ Depending on PID_v as:$ps = PID_{v2} + h1(s.PID_{v1})$, $sps = PID_{v2} + h1(s.PID_{v1})$.

a) RSU send ($ps\ or\ sps$) to TAS.
b) TAS will detect the real identity of this vehicle according to the registration record inside TAS.
c) If any illegal identity is detected, TAS will delete this registration from record and send (acknowledgment) to all RSUs in VANET
d) When RSU receive the (acknowledgment) from TAS, RSU will prevent this vehicle from renewing its signature. However, revoke operation can take effect after $T_{sk}\ expired$.

5. SECURITY ANALYSIS AND EXPERIMENTAL RESULTS

To prove that our proposed scheme is true and strong against well-known attacks we will take in this section two types of proofing the first about mutual authentication equations and the second for security analysis.

5.1. Mutual authentication prof

The first prof is for the equations used in the proposed scheme, the first equation will discussed is the **signature renewal** (1).

$$\sigma_v P = h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk}).pubk + h2(PID_{vn1} \parallel PID_{vn2} \parallel T_{s1})PID_{v1}$$

Taking L.H.S:

$$\begin{aligned}
&\sigma_v = SI + r.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_{sk}) \;\&\; SI^{new} = s.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_{sk}) \text{ Then:}\\
&= S.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk}) + P.r.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_1)\\
&= \big(P.r.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_1)\big) + \big(P.S.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\big)\\
&= \big(PID_{v1}.h2(PID_{vn1} \parallel PID_{vn2} \parallel T_1)\big) + \big(pubk.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\big)\\
&= \text{R.H.S.}
\end{aligned}$$

An accurate result is obtained from previous proofing. According to the proposed scheme, the recipient uses (2) to verify beacons in single verification operations.

$$\begin{aligned}
&\sigma_m.P = h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\, pubk + \omega \qquad (2)\\
&\sigma_m = (SI + r.h3(m \parallel T)) \;\&\; SI = s.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\\
&\sigma_m.P = \big(P.r.h3(m \parallel T)\big) + (P.S.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk}))\\
&= \big(PID_{v1}.h3(m \parallel T)\big) + pubk.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\\
&= \omega + pubk.h2(PID_{v1} \parallel PID_{v2} \parallel T_{sk})\\
&= R.H.S
\end{aligned}$$

According to (2), the result is accurate and can be used effectively. According to (3), which used for (n) beacons batch verifications.

$$\begin{aligned}
&P.(\textstyle\sum_{i=1}^{n}(x_i.\sigma_{mi})) = (\sum_{i=1}^{n}(x_i.\omega_i) + pubk(\sum_{i=1}^{n}(x_i.h2\big(PID_{iv1} \parallel PID_{iv2} \parallel T_{i,sk}\big)) \qquad (3)\\
&\text{For L.H.S } P.(\textstyle\sum_{i=1}^{n}(x_i.\sigma_{mi}))\\
&\sigma_m = SI + r.h3(m \parallel T)\\
&\sigma_m = P.(\textstyle\sum_{i=1}^{n}\Big(x_i.\big(SI + r.h3(m \parallel T)\big)\Big)\\
&\because SI = S.h2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,sk})\\
&= P.(\textstyle\sum_{i=1}^{n} x_i.((r_i.h3(m_i \parallel T_i) + (S.h2\big(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,sk}\big))))\\
&= \textstyle\sum_{i=1}^{n}((P.x_i.r_i.h3(m_i \parallel T_i)) + (P.S.x_i.h2\big(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,sk}\big)))\\
&= \textstyle\sum_{i=1}^{n}(\omega_i.x_i) + (x_i.pubk.h2\big(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,sk}\big))\\
&= (\textstyle\sum_{i=1}^{n}(x_i.\omega_i)) + pubk.(\sum_{i=1}^{n} x_i.h2\big(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,sk}\big))\\
&= R.H.S\ \boldsymbol{The\ (3) is\ occurate\ for\ batch\ verifcation}
\end{aligned}$$

5.2. Privacy preservation

There are three types of pseudonym in the proposed scheme: one for normal cars; and two for urgent/non-urgent emergency cars (for the COVID-19 virus), respectively. In all procedures, privacy preservation is achieved by concealing the real identity and using a pseudonym. A unique element denotes the real identity (RID_v), which is TAS. The pseudonym is computed inside TAS, using $ps = h3(RID_v \| r)$ for normal cars and $sps = h3(RID_v \| r)$ for emergency and team cars contributing to combatting the COVID-19 epidemic. It is also used to calculate PIDs and to broadcast it within beacons. An adversary cannot re-compute the real identity of a vehicle based on PIDs, even if it stole RSUs. Thi s is because the PID calculation involves $PID_{V1} = r.P$, $PID_{V2} = ps \oplus h1(r.pubk), PID_{V1} = r.P, PID_{V2} = sps \oplus h1(r.pubk)$, for normal and emergency vehicles, respectively. In this case, $r \in z^q$. Additionally, in signature renewal for normal cars, an adversary that has compromised RSUs can receive beacons. It is impossible to discover the real identity, meaning that- in view of the above- the proposed scheme preserves privacy.

5.3. Traceability and revocation proof

The following points articulate the proof of traceability and revocation for the proposed scheme:

a) Emergency and COVID-19 teams do not broadcast beacons for other OBUs.
b) All normal vehicles broadcast beacons for OBUs and RSUs. A beacon does not contain any information about the real identity. As illustrated in the revocation phase, TAS can trace and revoke any vehicle that broadcasts compromised beacons. The proposed scheme satisfies the tracing and revocation requirements.

5.4. Resistance against well-known attacks

Because the proposed scheme depends on mutual authentication, the MITM attack cannot take any effect. Any adversary needs to forge beacons that connect between the sender and receiver, which is impossible. The proposed scheme is very strong against reply and denial of service DOS attacks. Any continue beacons transferred among VANET systems have a timestamp that appoints the expired time.

6. PERFORMANCE EVALUATION

This section will describe both computation and communication cost.

6.1. Cost

The performance of our proposed scheme will be explained by comparing with jianhong [17], D. HE. et al. [18], L wu et al. [19], and J. CU. et al. [20]. This comparison is for computation cost. We note that [17] use bilinear pairing in cryptography operations, while [18-20] use ECC in cryptography operations. Bilinear pairing is based on an 80-bit length security level, additive group ($\underline{G}$) is generated depending on the ECC equation ($\underline{G}: y^2 = x^3 + x \ mod \ \underline{p}$)which uses ($\underline{p}$) of a 512-bit prime number. While these protocols use ECC has the same security level but depends on the equation ($G: y^2 = x^3 + ax + b \ mode \ p$) and uses (p=160 bit). To simplify the understanding of the current section we will use the following notation: Abbr, BGS, SBVO, and MBVO refer to abbreviation of cryptography operations, beacons generation and signing, single beacon verification operations, and multi beacons verification operations respectively. We must explain that we will exclude the execution time of XOR and concatenation because it is very small and can be neglected. Jianhong et al. [22], proposed a scheme its BGS operations include the following stages: four hash functions, one map-to-point hash function, two additions point, six numeric multiplications. If we calculate BGS time for this scheme, we note that total time is $(4T_{hf} + 1T_{m-p} + 2T_{ap} + 6T_{nm})$which approximately equals to (14.8313). SBVO operations include the following stages: two numeric multiplications, three bilinear pairing, three hash functions, and one additions point. The time calculation is $(2T_{nm} + 3T_{bp} + 3T_{hf} + 1T_{ap})$which is approximately equal to (16.2334). Finally, MBVO involves: (n+1) numeric multiplication, (2n) small numeric points, (3n-2) additions point, (3n) hash function, and three bilinear points. The summation of time is $\left(3T_{bp} + (n+1)T_{nm} + (2n)T_{smp} + (3n-2)T_{ap} + (3n)T_{hf}\right)$it is approximately equal to (1.9313n+14.2136). The scheme proposed by HE. et al. [23] , BGS involved the following operations: three hash functions, and three numeric multiplications. Hence, the overall BGS computation will be $(3T_{hf} + 3T_{nm})$ which approximately equal to (1.4223). SBVO operations are: two point additions, two hash functions, and three numeric multiplications, the computation equation will be $(2T_{pa} + 2T_{hf} + 3T_{nm})$ which approximately equal to (1.3329). While MBVO operations are: (2n) small number multiplication, (2n-1) addition point, (n+2) numeric multiplication, and (2n) hash functions, so the computation is $((2n)T_{snm} + (2n-1)T_{ap} + (n+2)T_{nm} + (2n)T_{hf})$ and the result is approximately equal to (0.5012n+0.7882). The scheme proposed by L wu et al. [24], BGS involved the following operations: two hash functions, and two numeric multiplications. Hence, the overall BGS computation will be $(2T_{hf} + 2T_{nm})$ which is approximately equal to (0.8833). SBVO operations are: two point additions, two hash functions, and four numeric multiplications. And the computation equation will be $(2T_{pa} + 2T_{hf} + 4T_{nm})$ which is approximately equal to (1.7381), while MBVO operations are: (2n+2) numeric multiplication, (2n) small number multiplication, (2n+1) addition point, and (2n) hash functions, so the computation is $(2n+2)T_{nm} + (2n)T_{snm} + (2n+1)T_{ap} + (2n)T_{hf})$ and the result is approximately equal to (0.9054n+0.8687).

The scheme proposed by J. CU. et al. [25] has the following operations for BGS: two hash functions, and two numeric multiplications, so the computation cost will be $\left(2T_{hf} + 2T_{nm}\right)$. The result is approximately (0,8644). SBVO comprises two numeric multiplication, two hash functions, and one additions point. Hence $\left(2T_{nm} + 2T_{hf} + T_{ap}\right)$ is the computation cost equation and it is approximately equal to (1.3381). While MBVO computations equation is $\left(2T_{nm} + (2n)T_{spm} + (2n+1)T_{ap} + (n)T_{hf}\right)$ because it

involves two numeric multiplication, (2n) small point multiplications, (2n+1) additions point, and (n) hash functions, and the result is approximately equal to (0.4888n+0.8734). Finally, we discuss our proposed scheme computation cost. BGS includes the following operations: two hash functions, and one numeric multiplication. So, the computation equation is $(2T_{hf} + 1T_{nm})and\ the\ result\ is$ (0.4233). SBVO calculations are $(2T_{nm} + 1T_{hf} + 1T_{ap})$ because it involves the following operations: two numeric multiplications, one hash function, and one additions point, and the result is approximately equal to (0.8765). While MBVO calculation equation constructed from: two numeric multiplication, (2n) small numeric multiplication, (n+1) additions point, and (n) hash function, the equation is $(2T_{nm} + (2n)T_{snm} + (n+1)T_{ap} + nT_{hf})$. Hence the result of MBVO computation cost is approximately (0.03001n+0.9211). Table 3 show the improvement of our proposed scheme in all computational costs with the other discussed schemes. Figure 4 illustrates the computation cost for all studded schemes and our proposed scheme with different number of beacons.

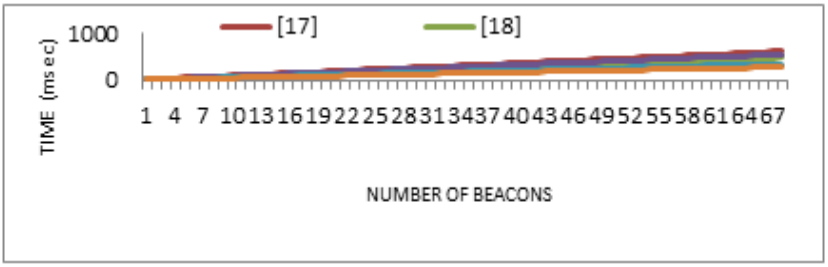

Figure 4. computation cost for different number of beacons

Table 3. Improvement of the reposed scheme

Scheme	BGS and BGS improvement of our scheme		SBVO and SBVO improvement of our scheme		MBVO and MBVO improvement of our scheme (for 50 beacons)	
	BGS	Improvement (0.4232) (%)	SBVO	Improvement (0.8765) (%)	MBVO	Improvement (2.4020) (%)
Jianhong et al. [22]	14.8313	97.14657515	16.2333	94.60060493	2.4112	0.381552754
HE. et al. [23]	1.4223	70.24537721	1.3329	34.24112837	2.6766	10.25928417
L wu et al. [24]	0.8833	52.08875807	1.7381	49.57137104	2.5644	6.332865388
J. CU. et al. [25]	0.8644	51.04118464	1.3381	34.49667439	2.4454	1.774760775

6.2. Communication cost

This section will compare between jianhong [22], D. HE. et al. [23], L wu et al. [24], and J. CU. et al. [25] schemes and our proposed scheme term of communication cost to find the overall overhead of our proposed scheme. As explained in the computation cost section, $\bar{p}$ size is 64-bytes, therefore the size of $\bar{G}$ will be 128-bytes. Also, size of p is 20-bytes and the size of G therefore will be 40-bytes. We assume time stamp size as 6-bytes, hash function to be 24-bytes, and assume elements in group integers to be 26-bytes. The Table 4 illustrates the communication cost for all mentioned schemes, we exclude the beacon inside content from our calculation. Jianhong [22], proposed a scheme with beacon size of (128*3+6) which equal to 390-bytes. This beacon includes three elements in $\bar{G}$, and one time stamp. HE. et al. [23], proposed a scheme its beacons of (40*3+26+6)=152 bytes. Beacon involves three elements in G, time stamp, and one elements in z_q. L wu et al. [24], argue that beacon size consisted from three elements in G, one hash function, and two time stamp. So, the size of beacon will be (40*3+24+10)=154 bytes. J. CU. et al.[25], decided the beacons size to be (40+(26*2)+6)=98 bytes. This beacon involved two elements in z_q, one time stamp, and one elements in $\bar{G}$. In our proposed scheme, we note that the beacons contain one element in $\bar{G}$, three elements in z_q, and one time stamp. Beacon size will be (40+ (3*26)+(2*6))=130 bytes. As shown in the previous calculations, our scheme possesses big overhead compared with the other schemes.

Table 4. Schemes communication cost

Scheme	Communication cost
Jianhong et al. [22]	390
HE. et al. [23]	152
L wu et al. [24]	154
J. CU. et al. [25]	98
Our scheme	130

7. CONCLUSION

This paper suggests a new spurious-ID based scheme in VANET with conditional pseudonym, integrity and message authentication. The proposed scheme uses a pseudonym instead of the vehicles real identity. The generation of this alternate identity depends on vehicles classification if normal or emergency. The proposed scheme satisfies all the privacy and security requirements and resisting the common attacks in VANET. The suggested scheme provides conditional anonymity in which if any vehicles conducting malicious then its real identity will uncover. Our scheme does not require the convention operations that are produced by a bilinear pairing operation. So, the proposed scheme able to conquer most of drawbacks of ID-based schemes. The preserve privacy in terms of the vehicle's real identity even from an insider attacker is one of the important characteristic. Furthermore, the TA can trace a dummy vehicle and revoke it as a member of the VANET. In addition to the proposed role in the process of expediting the arrival of medical teams (especially for COVID-19) and any vehicle bearing an emergency status by giving them the privilege to use the road and suggest alternative lanes in the event of a breakdown or interruption of the roads. A security analysis shows that the scheme is secure under the random oracle module and meets the security and privacy conditions of a VANET. We compare our scheme with related ID-based schemes that our scheme has computation costs lower than previous schemes and lightweight communication.

REFERENCE

[1] Qu, F., et al., "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985-2996, 2015.

[2] Al Shareeda, M., A. Khalil, and W. Fahs, "Realistic heterogeneous genetic-based RSU placement solution for V2I networks," *Int. Arab J. Inf. Technol.*, vol. 16, no. 3A, pp. 540-547, 2019.

[3] Jabbarpour, M.R., et al., "Applications of computational intelligence in vehicle traffic congestion problem: a survey," *Soft Computing*, 2018. 22(7): pp. 2299-2320.

[4] Bayat, M., et al., "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless networks*, pp. 1-16, 2019.

[5] Huang, J.-L., 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, 2010.

[6] Long, S., "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512," in *Journal of Physics: Conference Series*: *IOP Publishing*, 2019.

[7] Ahmad, I. and A.S. Das, "Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs," *Computers & Electrical Engineering*, vol. 31, no. 6, pp. 345-360, 2005.

[8] NIST, U., "Descriptions of SHA-256, SHA-384 and SHA-512," *Technical report*, 2001.

[9] La, V.H. and A.R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey, 2014.

[10] Raya, M. and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39-68, 2007.

[11] Lu, R., et al. "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*: IEEE, 2008.

[12] Zhang, C., et al. "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *2008 IEEE international conference on communications*, IEEE, 2008.

[13] Rajput, U., F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770-7784, 2016.

[14] Ming, Y. and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mobile Information Systems*, 2019.

[15] Zhang, L., et al., "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562-2574, 2015.

[16] Zhang, L., et al., "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516-526, 2016.

[17] Zhang, C., P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless networks*, vol. 17, no. 8, p. 1851, 2011.

[18] Lee, C.-C. and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless networks*, vol. 19, no. 6, pp. 1441-1449, 2013.

[19] Vijayakumar, P., et al., "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, 2015.
[20] Wang, S. and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Computer Communications*, vol. 112, pp. 154-164, 2017.
[21] Ali, I., T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *Journal of Systems Architecture*, vol. 103, p. 101692, 2020.
[22] Jianhong, Z., X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16, no. 5, pp. 351-358, 2014.
[23] He, D., et al., "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015.
[24] Wu, L., et al., "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, pp. 1550147717700899, 2017.
[25] Cui, J., et al., "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283-10295, 2017.