Journal of Communication Engineering (JCE)

P- ISSN: 2322-4088 Vol. 11, No. 1, Jan.-Jun. 2022 E- ISSN: 2322-3936

An Efficient Proxy-based Message Authentication Framework in Vehicular Ad-hoc Networks

Maryam Rajabzadeh Asaar* **[Corresponding Author]** Department of Electrical and Computer Engineering; Science and Research Branch; Islamic Azad University; Tehran, Iran Email: asaar@srbiau.ac.ir

Pouya Derakhshan-Barjoei Department of Electrical Engineering; Artificial Intelligence and Data Analysis Research Center; Science and Research Branch; Islamic Azad University; Tehran, Iran Email: pouya.derakhshan@srbiau.ac.ir

Received: *29 Feb. 2022* ***Revised:*** *16 Apr. 2022* ***Accepted:*** *14 Jun. 2022*

Abstract: In the recent research on Vehicular Ad-hoc Networks (VANETs), new practical goals are pursued. They provide real-world communications between vehicles and make them reliable and easily used. The VANETs have a fundamental role in reducing traffic accidents and improving traffic on the roads. Authentication in VANETs is a critical security service, and vehicles should be protected from breaking their personal information. Vehicles can be traced and investigated in the event of an accident or liability arising out of non-repudiation when the vehicle is faced with a rush of incoming messages. Hence, the Roadside Units' (RSUs) efficiency is reduced and causes delays in checking messages. This study presents an authentication framework using proxy vehicles for VANETs. Reducing the computational cost and proficiency increment are the features of the proposed method on the RSUs side. The proposed framework supports managing the revocation list. The Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) authentication protocols are guaranteed and designed in this proposed framework, therefor, a merged V2I and V2V authentication is presented and embedded in the proposed framework. The designed protocol applies offline and online signatures to check messages, the revocation key to prevent malicious messages from being sent, and the time limit to use the network. The analysis shows that the suggested protocol is more feasible and reasonable for use in VANETs.

Index Terms: Authentication, Proxy Vehicle, Privacy-preserving, Revocation Key, Vehicular Ad-hoc Networks.

Citation: P. Derakhshan-Barjoei and M. Rajabzadeh Asaar, "An Efficient Proxy-based Message Authentication Framework in Vehicular Ad-hoc Networks," *Journal of Communication Engineering*, vol. 11, no. 1, pp. 111-136, Jan.-Jun. 2024.

http://dx.doi.org/10.22070/jce.2024.18230.1255

I. INTRODUCTION

Most recently, as the population has grown, a wide range of vehicles has been used. Accordingly, the number of accidents that have caused irreparable damage has been increased. Different safety systems have been developed to prevent and reduce accidental injuries. One of these systems is the Vehicular Ad-hoc Network (VANET). The VANET has the potential to enhance the safety of transportation dramatically. The VANET is a new technology introduced under the assumption that the network nodes are moving cars, like a Mobile Ad-hoc Network (MANET), and providing communications between them and Roadside Units (RSUs) [1]. It is similar to the MANET in that it converts each device into a wireless router or a node, allowing them to connect at distances of 100 to 300 meters, which creates a widespread network [2,3]. The demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications has been steadily increasing. It is believed that VANETs are used for a wide range of safety enhancements such as accident alerts and traffic information and non-safety applications such as road conditions and mobile entertainment; according to the expectancy of accidents and exigent situations in life, the secure exchange of information between vehicles is vital [4]. Security issues have attracted much attention at VANET. Authentication is known as an important security service for VANETs in both V2V and V2I communications. To achieve security and privacy issues in VANETs, authentication protocols are divided into two categories: symmetric key cryptography (SKC) and public-key cryptography (PKC). The proposed protocols [5-8] use SKC for authentication. The disadvantage of using symmetric key management is that the vehicles have to authenticate each other through trusted authorities. This issue is not suitable for a high number of communications in VANETs. Authentication protocols using PKC are divided into public key infrastructure (PKI)-based and ID-base. The PKI-based protocols need access to infrastructure to obtain new keys, key certificate verification, and key revocation. Although various PKI-based authentication protocols have been proposed [4-7], these protocols require additional communication to manage revocation certificates. This may result in high communication and computation costs. ID-based authentication protocols [15-22] have been proposed to reduce computational costs and communication overheads using the vehicles' identity encryption and digital signature verification.

Due to the high importance of the speed of transport operations on RSU sides in VANETs, there is intense competition among VANETs' security protocols. Contribution: As the main contribution, this study presents a new framework for authentication that improves efficiency and reduces the computational costs on the RSU side. As the shadow contribution, an authentication protocol to embed in the proposed framework is designed. The designed protocol uses online and offline signatures in VANET for this purpose. Moreover, the vehicles need revocation keys to use

the network. The mentioned contributions are mentioned shortly:

- ◇ An impressive framework for message authentication and message recovery using proxy vehicles suitable for VANETs is presented. The proposed framework connects in-range vehicles to RSU using proxy vehicles. However, vehicles' privacy is kept.
- ◇ In the presented framework, sent messages can be authenticated and recovered.
- ◇ The presented framework also supports managing the revocation list, and misbehaved vehicles will be revoked from the network if needed (the TA revokes misbehaved vehicles based on receiving protest reports received from RSU).
- ◇ The presented framework is designed so that it can support V2I and V2V authentication protocols.
- ◇ To show the previous claim and as a practical example, an authentication protocol that includes V2I and V2V authentication is designed and embedded in our proposed framework.

Analysis shows that despite the proposed protocol's performance, which is designed based on the presented framework, is not as efficient as the ID-MAP's performance [28], it supports managing the revocation list. However, the proposed protocol is more reliable than the PBAS [25] protocol, while it has the additional feature of managing the revocation list.

Organization: The rest of this paper is organized as follows:
Section II presents the related works. Section III presents the paper preliminaries, including notations, mathematics and complexity presumptions, and the proposed framework's definition. Section IV, as the main section of this study, proposes an efficient RSU-based message recovery framework using proxy vehicles that is suitable for VANETs. It then presents the proposed framework's security analysis. Section V evaluates and compares the presented framework, with the detailed protocol, to some recently proposed protocols.

II. RELATED WORKS

In 2002, Perrig et al. [8] introduced the TESLA broadcast verification protocol. The TESLA was a MAC-based efficient broadcast authentication protocol and provided a time synchronization between network nodes. Unfortunately, it allowed adversaries to trace the vehicles' path.

In 2008, Zhang et al. [15] proposed an ID-based signature protocol that supported batch verification to reduce authentication costs on the RSU side. In 2010, Sun et al. [12] proposed an anonymous authentication protocol based on hash chains in which vehicles' pseudonyms were replaced instead of their real identities. The size of the Certificate Revocation List (CRL) has grown exponentially to revoke most of the pseudonyms. Therefore, to reduce the CRL size, the

hash chain idea has been proposed by them. Although the proposed approach minimized the signature's computational cost, and the hash chain calculation incurred additional computational costs and did not properly address the process of reversing malicious devices.

In 2011, Chim et al. [10] investigated that the protocol presented by Zhang et al. [9] was not resistant to impersonation and privacy flaws attacks, and it was traceable. Therefore, a new ID-base authentication protocol is offered by using two shared private keys, as well as bloom filter and binary search techniques. Their protocol was highly pivotal in terms of communication cost and message endorsement by a factor of 45% compared to the protocol proposed by Zhang et al.

In 2012, Lu et al. introduced a newfound ID-based authentication framework with adaptive privacy preservation for VANETs [14], which was an ID-base protocol, as well as used the offline and online signature protocols (IBOOS) [23] and the ID-based signature protocol (IBS) [24].

In 2013, Wasef et al. introduced a protocol called "expedited message authentication protocol for vehicular Ad-Hoc networks" (EMAP) [13], that used public key infrastructures and CRL to verify whether the sender has revoked the received or not. This process was very time-consuming due to the large size of the CRL. To overcome this restriction, it used the hashed message authentication code key (HMAC) to substitute the CRL check process. It greatly reduces the checking time, but the telecommunication overhead was high.

In 2013, Lee et al. [18] explained that the protocol presented by Zhang et al. [15] was vulnerable to the replay attack, and they then modified it to provide an ID-base authentication protocol for vehicles while maintaining efficiency.

In 2014, Zhang et al. [19] analyzed Lee et al.'s protocol [18] and showed it was vulnerable to impersonation attacks and lacked the non-repudiation feature. Zhang presented a modified signature scheme [19] to improve the mentioned vulnerabilities. In the same year, Li et al. [22] proposed a general framework for vehicle authentication, in which privacy-preserving and non-repudiation were assumed as security requirements. The proposed protocol used Public-Key Cryptography (PKC) instead of vehicles' real identity, as well as this protocol was based on online and offline signature protocol [23] (IBOOS) and the ID-base signature (IBS) [24] protocol. Lee has tried to slow down the process of vehicle authentication, but its protocol speed was still not appropriate since RSUs have to check a large volume of messages; when the message volume was high. It caused bottlenecks on the RSU side and the message-checking operations' speed was decreased.

Another method of vehicle authentication protocol is to get help from proxy vehicles, as researched in 2015 by Liu et al. [25]. They proposed a protocol called message authentication using proxy vehicles in vehicular ad-hoc networks. Their protocol showed that using proxy

vehicles could reduce authentication process costs on RSUs.

In 2016, Malhi et al. proposed a scheme called the privacy-preserving authentication framework for VANETs [26]. The proposed framework used pseudonyms for communications. The mentioned protocol was designed based on a digital signature, and the batch verification method was provided. Therefore, designing efficient, secure, and low-cost vehicle authentication protocols for inter-vehicle networks remains a challenge.

In 2017, Yang et al., to solve the mentioned challenge, proposed a new ID-base authentication protocol for VANETs, which reduced 88% of the computational cost of message signature and verification [27].

In 2018, Asaar et al. [28] demonstrated in their protocol that Liu et al. [25] protocol was not secure and proposed an authentication protocol using a proxy vehicle to address its security vulnerabilities.

Some other message authentication protocols for VANETs have been proposed in the last three years. In 2019, Zhang et al proposed a message authentication protocol that used both group signature and group session key [33]. Their proposed message authentication protocol used the combination of batch group signature verification and group session key. In addition to reducing the number of pairing operations in their protocol, it resisted impersonation attacks. In the same year, Shen et al. proposed a data aggregation protocol that supported batch verification for real-time traffic data in VANETs [34]. In their protocol, the original traffic data was recovered successfully if the validity of received signatures from vehicles was verified. Additionally, batch verification was supported in their proposed protocol for multiple vehicles' messages while keeping confidentiality. Li et al.'s protocol supported hierarchical registration to prevent leaks of registration information and flimsy secret leakage attacks on the registration authority side [35]. The proposed protocol in [35] applied self-certified public keys and Schnorr signatures. It was shown that the protocol provided security in the random oracle model under the Diffie-Hellman assumption.

In 2020, Li et al. proposed a lightweight protocol for user authentication in VANETs under the security of the hash function [36]. The proposed lightweight protocol was suitable for VANETs that had high-speed mobility and needed to meet privacy-preserving. Mundhe et al. proposed a different message authentication protocol by applying a lattice-based ring signature to provide vehicles' privacy and security against quantum computers [37].

In 2021, Wang and Liu proposed another efficient message authentication protocol [38]. They claimed and solved that pseudonyms-based and group-based message signing have some downsides. Their presented message authentication protocol was aimed at approaching mutual

authentication among vehicles and RSUs. In 2020, Mahmoud et al. investigated an anonymous authentication protocol for adaptive client□server infrastructure [39]. An enhanced authentication scheme on elliptic curve cryptography studied by Bhuarya et al.[40]. In 2021, Sadri and Rajabzadeh proposed a hash□based authentication protocol with forward secrecy in WSN [41]. A hybrid framework for a multiple type of WSN has been done by Baskaran et al. in 2021[42]. In [43] Naresh et al. investigated a Lightweight secure communication system, in their research, a protocol based on message queuing transport telemetry for e□healthcare environments studied. Jiang et al. studied a scheme based on lightweight and privacy□preserving traffic monitoring in 2022[44]. the QoS challenges and MAC and PHY layered protocols enhancement studied to reach the optimal performance behind the design of Wireless MediaNets[45-47].

III. PRELIMINARIES

This section presents paper preliminaries; The list of notations is shown in Table 1.

A. Motivation

As this study's background, various message recovery protocols were checked. In most of them, vehicles are directly connected to RSUs and were sending their requests to. The misbehaved vehicles tried to implement the denial of service attack on the RSU side by applying many requests. They wanted to be present on the network to continue their misbehavior works. Many approaches and methodologies to prevent sending invalid requests and reduce sent load to RSAs have been presented. However, no unique method as their basic framework was considered.

The main problem that is sensed is the absence of a basic framework that can be assumed as the base of proxy-based message authentication protocols which reduces RSU side computational costs. Additionally, it is required to support managing the revocation list in which misbehaved vehicles are removed. Therefore, the main problem that this study concentrates on solving is defined as "the absence of an efficient framework that supports proxy-based message authentication protocols".

IV. THE PRESENTED FRAMEWORK

This section presents the definition of the framework that is presented atop the designed authentication protocol. The mentioned framework is shown in Fig. 1 and described in the following subsections.

Table 1. List of Notations

Notation	Definition
Nonce	The random number
RSU_i	The *i*-th roadside unit
V	A vehicle
V_p	A proxy vehicle
ID_r	The real identity of RSU.
PS_{p_v}	The pseudonym of the proxy vehicle
PS_{v_i}	The pseudonym of the vehicle
T	The timestamp for V2R and R2V authentication
T	The timestamp for V2V authentication
m_i	The invitation message for R2V authentication
m_j	The join request message
m_p	The updating or getting revocation key message
RK_i *or* RK_p	The revocation key
SIG, σ	The signature.
G	An additive group
P	The generator of the group G
s_1, s_2, s_3	System secret keys
β_r	The RSU's secret key
$R \xrightarrow{\$} r$	Assigning a uniformly random element of R to r
$P_{pub,1}$, $P_{pub,2}$	The system's public keys
V_i	The *i*-th vehicle
ID_i	The real identity of the *i*-th vehicle
V_p	The proxy vehicle
ID_p	The real identity of a proxy vehicle
$PS_{V_i} = (PS_{V_i,1}, PS_{V_i,2})$	The pseudo-identity of the *i*-th vehicle
β_{i_i}	The Vehicle's secret keys
m_i	The message sent by the vehicle v_i
m_p	The message sent by the proxy vehicle v_p
β_p	proxy vehicle's secret keys
σ^{online}, $\sigma^{offline}$	The online and offline digital signature
$\rightrightarrows$, $\rightarrow$	The broadcast and unicast communication.
$\circledast$	The vehicles in the range of RSU.

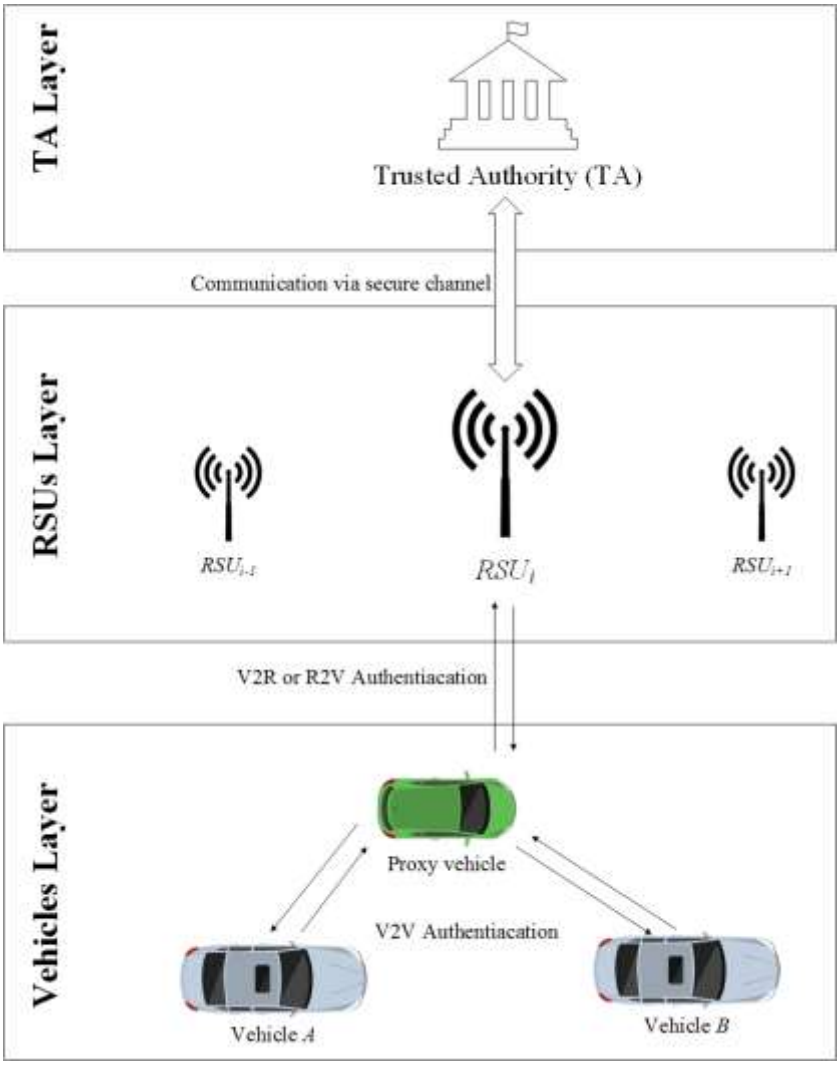

Fig. 1. The Presented Framework

A. Entities and Components

As shown in Fig. 1, the proposed framework involves three layers and four types of entities. Framework components, entities, entities' roles, and their position in the three mentioned layers are defined in the following:

- ◇ Trusted Authority (TA): The TA is a trusted third party responsible for the registration of RSUs and OBUs and generating and preloading factors. The TA can disclose the driver of a vehicle's identity in the event of any crime or accident (note that it is assumed that the TA's computation and communication capabilities are highly reliable). The TA can update the revocation list.
- ◇ Roadside Units (RSUi): The RSU is a fixed physical device for communication usually located at intersections and traffic lights and can provide the needed information to TA and

vehicles or proxy vehicles. They generate revocation keys and the related signatures offline.

- ◇ On-board Units (OBU): In VANETs, moving nodes are vehicles; each moving vehicle is equipped with a global positioning system and a Tamper-Proof Device (TPD) that checks and records speed, time, location, and other vehicle information in an emergency. Moving vehicles, which have extra computational resources, can be assumed proxy vehicles and help RSUs with authentication signals.
- ◇ Vehicles and proxy vehicles: They are regular network users who communicate together. The proxy vehicles, which have extra computational resources, could help RSUs with decreasing their computation costs and delays. They can be presented between two far vehicles and connect them or between a vehicle and RSU.

B. Definition

According to the defined framework entities and their roles, the framework consists of three main phases. They are defined briefly in the following:

1. System initialization: The system is initialized by the TA, and RSUs' and vehicles' keys are taken to them through a secure channel.
2. System pseudonym generation: The TA generates the secret values; The pseudonyms are then generated by TPD and assigned to vehicles.
3. The protocol phase: Two merged authentication protocols (V2I and V2V authentication protocols) are executed in this phase. This protocol creates a secure message authentication way across the vehicle and proxy vehicle (V2V) and then proxy vehicle to RSU (V2I).

C. Security Model and Design Goals

The essential security requirements for VANETs were specified in [19, 24, 26-27]. Their brief overview and definitions, matched with the presented framework, are presented in the following:

- ◇ Resistance to attacks on authentication: Authentication is done by two signatures, the first signature is done by the vehicle consisting of the offline signature on the pseudo-ID of each vehicle, and the second signature is done by the tamper-proof of the vehicle consisting of the first signature. The digital signature used is assumed; it cannot be forged. Also, adversaries cannot invalidate the authentication operation because they cannot calculate the offline signature generated by the roadside unit, and the second signature created by the tamper-proof device of the vehicle is forged.
- ◇ Resistance to attacks on privacy: To protect the privacy of vehicles, they use pseudo-identities in their communications, and other vehicles and RSUs are unable to manifest the

real vehicle identity of a specific message sender while confirming the message.

- ◇ Resistance to attacks on non-repudiation: Non-repudiation means, the vehicle can deny its message if it sends a message. Non-repudiation is achieved by encrypting real vehicle's identities with a private key. Since communication with a trusted authority or roadside unit is secure in this scheme, it can be argued that authorized third parties (e. g., the police) at any time can link pseudo-identities with the identity of a vehicle with a valid digital signature, which protects authorized persons against repudiation attacks.

The below goals should be achieved in the presented framework (after the framework description, it will be shown the presented framework achieves the listed goals).

- ◇ Message authentication: Satisfying authentication and integrity is the most important challenge in VANETs' protocols. The purpose of authentication is to assure the sender. Also, vehicles or proxy vehicles and RSUs should be capable of checking the integrity, authenticity, and validity.
- ◇ Identity privacy-preserving: The TA can obtain vehicles' real identities, and no one should be able to learn the real identity of vehicles.
- ◇ Unlinkability: On having two (or more) messages, vehicles or RSUs should not be able to learn whether or not they were sent by one vehicle.
- ◇ Traceability: The TA should be able to extract the real identity of a misbehaved vehicle or proxy vehicle and report it to the police.
- ◇ Resistance to common attacks: In addition to previous goals, a security protocol should also provide security against common attacks listed below:
  - ◆ Resistance to man-in-the-middle attack: In this type of attack, the attacker acts as an interface between the two vehicles communicating so that the two vehicles do not notice its presence. In addition to observing communications, it can also modify messages sent by the other vehicle.
  - ◆ Resistance to impersonation attack: In this attack, the attacker pretends that it is one of the network's legitimate users to reach its subversive target.
  - ◆ Resistance to the replay attack: In this attack, the attacker replaces previous messages instead of current messages.

V. THE FRAMEWORK

A. Detailed Framework

This section presents the detailed proxy-based framework, including three main phases: system initialization, system pseudonym generation, and protocol phases.

Table 2. R2V and V2R Authentication Phases

	Flows	Messages	Description
Phase 1	$RSU \rightrightarrows \circledast$	$\{ID_r, T_1, m_r, nouns, \sigma_r\ (ID_r \| T)\}$	RSU's information is broadcast.
Phase 2	V_i $Or \rightarrow RSU$ V_p	$\{ID_r, T_1, m_i, PS_{v_i}, \sigma_{v_i}\ (PS_{v_i} \| T)\}$ $\{ID_r, T_1, m_p, PS_{v_p}, \sigma_{v_p}\ (PS_{v_p}) \| T)\}$	A proxy vehicle or a vehicle authenticates itself to the RSU.
Phase 3	V_i $RSU \rightrightarrows Or$ V_p	$\{ID_r, t, Set_{v_i}\ (POR), nonce, \sigma_r\ (ID_r \| t)\}$ $\{POR = PS_{v_i} / \sigma_r^{offline} / RK_i\}$ $\{ID_r, t, Set_{v_p}\ (POR), nonce, \sigma_r\ (ID_r \| t)\}$ $\{POR = PS_{v_p} / \sigma_r^{offline} / RK_P\}$	RK_i or RK_p are broadcasted by the RSU.
Phase 4	$V_p \rightarrow RSU$	$\{ID_r, t_p, M, PS_{v_p}\ RK_p, \sigma_{v_p}\ (PS_{v_p} \| t_P \| M)\}$ $\{M = \sum_{i=1}^{n} m_i \| \sum_{i=1}^{n} t_i \| SIG_1 \| SIG_2\}$ $SIG_1 = \sum_{i=1}^{n} \sigma_1$ and $SIG_2 = \sum_{i=1}^{n} \sigma_2$	If a proxy vehicle is in the range of an RSU, it contributes to the RSU during the authentication process and sends the output result to the RSU.

1) System Initialization Phase

The TA first serves in a region, such as a city, a province, or a country. Ere entering into the covered region, each vehicle has to be registered to TA, and also, by registering a vehicle, TA submits the vehicle's specifications and identity. The TA preloads necessary information in all RSUs and vehicles through a secure channel. The number of RSUs usually is fixed, and identifications of RSUs are preloaded in each vehicle's tamper-proof (note that all communications between TA, RSUs, and Vehicles are done securely).

2) System Pseudonym Generation Phase

In this phase, on request of the vehicle that wants to update or generate its pseudonym $PS_{v_i} = (PS_{v_i.1} . PS_{v_i.2})$, the TA puts private keys in RSUs and vehicle's tamper-proof (to prevent replay attack, each vehicle can send periodically update request to fresh its pseudonym); also it broadcasts system's public keys periodically.

3) The Protocol Phase

Authentication in VANETs is done in three steps roadside-to-vehicle, Vehicle-to-Roadside (V2R), and Vehicle-to-Vehicle (V2V). In this framework, communications between vehicles should be managed securely, and all communications between TA, RSUs, and vehicles should be trustworthy. The RSUs periodically broadcast their information, and a proxy vehicle can help the RSU during the authentication process if it is in its region. Additionally, the vehicle that is using VANET has to update its revocation key at a specific time since it is valid for a limited time. Therefore, the TA

can revoke a malicious vehicle.

This process is described in detail in the following, and Tables 2 and 3 show the flow-based overview.

B. The V2R and R2V Authentication

In this phase, the authentication among RSU and vehicles is described in four phases.

Phase 1: At first, the RSU, for authenticating of V2R and R2V communications, broadcasts its information. A vehicle or a proxy vehicle, which is in its range, can get RSU's information {ID_r, T, m, nouns, SIG_r (ID_r‖T)}, where ID_r is the real identity of the RSU, T is the time stamp, m is the message invitation for authentication of V2R communications, nonce is a random number for freshness and SIG_r is an ID-based signature on ID_r and t for authentication of R2V communication.

Phase 2: A vehicle or a proxy vehicle receives the RSU's information if it is in the RSU broadcasting range and authenticates it through verification of the ID-based signature of the RSU. A vehicle or a proxy vehicle replies to the message to the RSU through one of the following cases if it makes sure the received message from RSU is valid.

- ◇ A vehicle or a proxy vehicle updates or generates a new pseudonym and wants to update or gets a revocation key from the RSU for authentication and communications in VANETs.
- ◇ A new RSU's identity is received by a vehicle or a proxy vehicle from the RSU's broadcast.

The new vehicle's or proxy vehicle's pseudonym is unicasted to the RSU by it in the message { ID_r, T1, mi, PS_{v_i}, $\sigma_{v_i}(PS_{v_i}$‖T)} if it is a regular vehicle and in the message {IDr, Tp, mp, PS_{v_p}, ($\sigma_{v_p}(PS_{v_p}$‖T)} if it is a proxy vehicle, where IDr is the real identity of the RSU, T1 is the time stamp, mi and mp are the request of join message and updating message or getting revocation key message respectively, $\sigma_{v_i}(PS_{v_i}$‖T) is the signature begot from the pseudonym of a vehicle, and $\sigma_{v_p}(PS_{v_p}$‖T) is the signature generated from the pseudonym of a proxy vehicle.

Phase 3: At first, the RSU verifies the received signature of a vehicle or a proxy vehicle, and it accepts it if it is valid. The RSU, after authenticating the message, saves a new pseudonym in its memory, and also new pseudonym of the vehicle is reported to the TA. The RSU then generates a new revocation key RKi for the newly served pseudonym PS_{v_i} and the expiry time Tj related to the vehicle Vi.

The RSU, after generating RKi broadcasts a message {IDr, t, Set_{v_i} (POR), nonce, σr(IDr‖t)} to all vehicles where IDr is the real identity of RSU, t is the time stamp, POR consists of a pseudonym PS_{v_i}, an offline signature and a revocation key RKi which are generated by the RSU,

Table 3. V2V Authentication

	Flows	Messages	Description
Phase 1	$V_{p\ or}\ V_i \rightrightarrows V_f$	$\{PS_{v_p.v_i}, t, m, nonce, RK_{i\ or\ p}, (\sigma_1), (\sigma_2)\}$ $\{\sigma_1 = \sigma_{v_p or\ v_i}^{online}(\sigma_{v_i or\ v_p}^{offline}(PS_{p\ or\ v}) \| t)\}$ $\{\sigma_2 = \sigma_{v_p or\ v_i}^{online}(\sigma_1 \| PS_{p\ or\ v} \| t \| h(m_i))\}$	The proxy vehicle or the vehicle i authenticates to vehicle f

the nonce is the random number and σr(IDr‖t) is RSU's signature on IDr and t. All vehicles at the RSU's range receive the message verify the signature, and save or update POR in their memory if it is a valid vehicle.

Phase 4: A proxy vehicle helps the RSU with message authentication if it is in the range of the RSU. The proxy vehicle unicasts the output result {IDr, tp, M, PS_{v_p}, RKp, $\sigma_{v_p}(PS_{v_p}\|t1\|M)$} to the RSU, where IDr is the identity of the RSU, tp is the time stamp, M is $\{\sum_{i=1}^{n} m_i \parallel \sum_{i=1}^{n} t_i \|SIG1\|SIG2\}$, where $\sum_{i=1}^{n} m_i$ is the sum of the valid messages of vehicles, $\sum_{i=1}^{n} t_i$ is the sum of time stamps, RKp is revocation key, SIG1 is the aggregation of the online signatures of vehicles that includes time stamp and a pseudonym of a vehicle and SIG2 is the aggregation of the vehicle online signatures of vehicles that consists of σ1, time stamp and a pseudonym. Also, $\sigma_{v_p}(PS_{v_p}\|tp\|M)$ is the proxy vehicle's signature on PS_{v_p}, tp, and M (note that the method for selection of a proxy vehicle is given in Asaar et al. 's protocol [28]).

C. V2V authentication

For V2V authentication, the vehicle broadcasts the message $\{PS_{v_i or v_p}$, t, m, nonce, RKi or p, σ_1, $\sigma_2\}$ to all vehicles in its transmission range. The vehicle firstly generates the first online signature σ_1 from the offline signature which has been generated by the RSU and time stamp; secondly, it generates the second online signature $\sigma_{v_i.2}$ that consists of the first online signature, a pseudonym, and the time stamp and m is a message about traffic, accident and etc, t is a time stamp and nonce is random.

For V2I authentication, at first, the vehicle or the proxy vehicle checks if Vi for $1 \le i \le n$ has not been revoked. To do this, it checks the freshness of the received message using RKi and checks timestamp t and the validity of pseudo identities. It then checks the validity of the two signatures σ1 and σ2 and accepts the received message if they are valid; Otherwise, it drops and reports to RSU.

As aforementioned in Phase 4 of V2R authentication, the proxy vehicle will perform the authentication operation if it is in that area.

D. Detailed Protocol

The mentioned V2I and V2V authentication protocol, which was said to be embedded in the presented framework, will now be described below in seven phases.

1) Setup

The TA generates parameters of the system and preloads them into the vehicle's tamper-proof devices (TPD) and RSUs. The initialization phases are as follows:

- ◇ The TA chooses two large prime numbers p and q and the elliptic-cure E over a prime finite field Fq that is defined as E: y2= x3+ ax+ b where a, b ∈ Fq such that Δ= 4a3+ 27b2≠ 0.
- ◇ It then selects P as the generator of additive group G with order q, in which G consists of all points on the elliptic curve E and the point at infinity O.
- ◇ The TA chooses three random numbers s1, s2, s3 ∈ Zq* as the system's secret keys and computes the two system's public keys Ppub,1= s1P and Ppub,2= s2 P.
- ◇ The TA chooses five secure hash function f(.), g(.), h(.), H(.) and k(.), where f(.), g(.), h(.), H(.), k(.) are defined as {0,1}*→ Zq*.
- ◇ The TA chooses xr $\xleftarrow{\$}$ Zq* for computing the RSU's identity ID and generates IDr,1= xr P, IDr, 2= ID, and IDr= (IDr,1, IDr,2). It then computes βr= xr+ s1 f (IDr) mod q as the RSU's secret key.
- ◇ The TA puts the system's public parameters {G, q, P, Ppub,1, Ppub,2, f(.), g(.), h(.), H(.), k(.)} into all RSUs' and vehicles' memories. Additionally, it preloads the tamper-proof device of each vehicle with {IDi, s1, s3, IDr, βr} and it preloads RSU's with {s2, βr} (the mentioned processes are done securely).

2) Pseudo-identity Generation

To satisfy privacy the vehicle's secret key is generated. At first, the tamper-proof of each vehicle selects a random number xi ∈ Zq* and computes $PS_{v_i.1}$= xi P, $PS_{v_i.2}$= IDi ⊕ g(xi Ppub,2) ⊕ g(s3) to reach the pseudo-identity PS_{v_i}= ($PS_{v_i.1}$, $PS_{v_i.2}$). Then, it computes the vehicle's secret key βi= xi+ s1 g (PS_{v_i}) mod q and gives (βi, PS_{v_i}) to the vehicle through a secure channel.

3) Revocation Key Generation by RSUs

In this phase, the RSU checks the revocation lists RLs. The RSUs periodically catch updated RLs from the TA and it computes RKi= g(Tj) ⊕ g(s2 PS_{v_i},1), Tj ∈ Z_q^* as the secret key that is shared between non-revoked vehicles by RSU if IDi ⊕ g(s3) is not found in the RLs. It is valid in the specific time interval and is updated because of the time goes on (e.g., Tj+ 1, Tj+2, …). The RSU chooses w ∈ Z_q^* as a random number and computes W= w P, hr= h(PS_{v_i} ‖ W), U= hr w+ RKi β_r mod q and sends (U, RKi, W) to the vehicle.

4) Message Generation by Vehicles

A vehicle picks a random number zi $\in Z_q^*$ and computes Zi= zi P, Hi= H(mi‖PS_{v_i} ‖Zi‖ti) and σ_i,1= zi Hi+ Ui+ β_r mod q and gives $\sigma_{i.1}$, mi, ti to the tamper-proof device where ti is the timestamp. The tamper-proof first calculates RKi ⊕ g(xi P_{pub},2) to generate g(Tj) since g(xi P_{pub},2)= g(s2 PS_{v_i},1) (note that an adversary and a vehicle cannot compute g(Tj) since the CDH problem is computationally hard). Then, the tamper-proof device selects ri as a random number from Z_q^* and computes ri P= Ri, ki= k(mi‖ti‖PS_{v_i} ‖Ri) and σ_i,2= s1(ki+ σ_i,1)+ ri+ xi mod q and sends {PS_{v_i}, ti, mi, Ri, Zi, W, RKi, $\sigma_{i.1}$, $\sigma_{i.2}$ } to proxy vehicles in its vicinity.

5) Batch Verification

In this phase, each proxy vehicle, which has not been revoked, can verify messages and then send the result of message verifications to the RSU. The proxy vehicle first checks if Vi ($1 \leq i \leq n$) has not been revoked. To do this, it checks the received message's freshness by RKi and gets g(Tj) from RSUs. The tamper-proof of each proxy vehicle generates g(s2 PS_{v_i},1) as RKi ⊕ g(Tj)= g(s2 PS_{v_i} ,1) as a result, the tamper-proof of the proxy vehicle gets g(xi Ppub,2) for $1 \leq i \leq n$, then it checks timestamp ti and checks the validity of pseudo identities. The proxy vehicle then computes H=Hi(mi‖ PS_{v_i}‖Zi‖ti), gi= g (PS_{v_i},1), hr= h(PS_{v_i}‖W) and checks ($\sum_{i=1}^{n} a_i \sigma_i$,1) P= $\sum_{i=1}^{n} (a_i H_i) Z_i$+ $\sum_{i=1}^{n} (a_i h_r) W + \sum_{i=1}^{n} a_i ID_{r.1} RK_i + \sum_{i=1}^{n} (a_i P_{pub.1} RK_i) f(ID_{r.1}. ID_{r.2}) + \sum_{i=1}^{n} a_i PS_{v_i.1}$

$\sum_{i=1}^{n} (a_i g_i)$ P_{pub},1 gi. (1)

All received signatures σ_i,1 are valid if Equation (1) holds. Hence, $SIG_1 = \sum_{i=1}^{n} \sigma_i$,1, calculated by the proxy vehicle. After that, the proxy vehicle obtains ki= k (mi‖ti‖$PS_{v_i.1}$‖Ri). Then, it checks ($\sum_{i=1}^{n} a_i \sigma_i$,2) P=$\sum_{i=1}^{n} a_i (k_i + \sigma_1)$ Ppub,1+ $\sum_{i=1}^{n} a_i R_i$+ $\sum_{i=1}^{n} a_i PS_{v_i}$,1 (2)

The signatures σ_i,2 are valid if Equation (2) holds; and the proxy vehicle computes SIG_2=$\sum_{i=1}^{n} \sigma_i$,2. The proxy vehicle sends {c,PS_{v_p}, PS_{v_i}, Ri, ti, SIG_1, SIG_2, Zp, σ_p} to the RSU, where c is the verification result generated by the proxy vehicle. c= 0 if the batch result is valid; Otherwise c= 1. The proxy vehicle's signature is σ_p= $z_p h_p$+ U_p+ β_p mod q, where H_p= H (mp‖PS_{v_p}‖tp‖Zp), mp= (c, PS_{v_p}, PS_{v_i}, Ri, ti, SIG_1, SIG_2) and Up= hr w+ RKp β_r mod q.

6) Verification Proxy Vehicle's Output by RSU

In this phase, RSUs can verify the proxy vehicle's output find false results, and revoke malicious proxy vehicles. The verification details by RSUs are done as follows:

◇ At first, the RSU checks message integrity and the sender's identity by verification of the proxy vehicle's signature. The RSU rejects the message if the signature is invalid;

Otherwise, the RSU goes to the next step.

The verification equation is written as $\sigma_p P$= zp Hp+ hr w+ ID_r,1 RKp+ P_{pub},1 RKp f (ID_r,1. IDr,2)+ $PS_{v_p.1}$+ Ppub,1 gp (3)

and Hp= H(mp‖PS_{v_p}‖Zp‖tp), gp= g($PS_{v_p.1}$) and hr= h(PS_{v_p}‖W).

- ◇ The RSU then checks the message's freshness using ti and the pseudo identities' validity. It goes to the next step if they are valid; Else it rejects the received message.
- ◇ The RSU verifies SIG_2 if Equation (4), written in the following, holds and sets c= 1. The RSU asks TA to revoke the malicious proxy vehicle if Equation (6) is not held.

SIG_2P= $((\sum_{i=1}^{n} k_i) + SIG_1)\, P_{pub}$,1+ $\sum_{i=1}^{n} R_i + \sum_{i=1}^{n} PS_{v_i}$,1 (4)

7) Management of Revocation Lists

The proxy vehicle finds the vehicle that sent incorrect information, so a proxy vehicle sends a protest to its nearest RSU. On receiving the protest, the RSU sends the TA's protest and asks it to revoke the malicious vehicle.

For managing revocation lists, the TA updates them in specific time intervals and gets a protest message from an RSU before updating time reaches. The RLs are published in all the RSUs by TA, and then RSUs give tokens to the vehicles that are not in RLs.

It is assumed that the TA gets a message of protest for the vehicle Vf. The TA uses s2, s3, and the malicious vehicle's pseudo-identity PS_{v_f} to find its real identity .The TA sends important information to an executive authority for punishment, sets IDf ⊕ g (s3) (5)

The vehicle Va wants to compute the token Tj, so it sends a request to join (RJ) or a request for a token (RT) to the nearest RSU. Like Phase 4, the vehicle Va picks a random number za ∈ Z_q^* and computes Za= za P, Ha= H(ma‖PS_{v_a}‖Za‖ta) and $\sigma_{a.1}$= zaHa+ Ua+ $\beta_a$mod q, where ma= RT or RJ and sends $\sigma_{a.1}$ to the RSU. The RSU generates Ha= H(ma‖PS_{v_a}‖Za‖ta), ga= g(PS_{v_a}), hr= h(PS_{v_a}‖W), and then it checks whether or not the following equation holds.

σ_a,1 P= Za Ha+ hr W+ RKa(IDr+ Ppub,1 f(IDr,1, IDr,2)) + PS_{v_a},1+ Ppub,1 ga (6)

The RSU checks RLs the same as Phase 3 and gives RKa to the vehicle and a vehicle's tamper proof similar to Phase 4 generates g (Tj) if Equation (6) holds; otherwise the RSU ignores the message.

E. Security analysis

This section analyzes the designed protocol's security matched to the presented framework.

1) Message authentication

In the proposed protocol, two signatures $\sigma_{i.1}$. $\sigma_{i.2}$ are applied to verify the authenticity of messages transmitted from vehicles to proxy vehicles. The authenticity of messages and vehicle's identities are checked by proxy vehicles, where the signature $\sigma_{i.1}$ is generated by the vehicle's private key β_i and the signature $\sigma_{i.2}$ is generated by the RSU's private key β_r and signature $\sigma_{i.2}$ is produced by the tamper-proof device with the system's secret key s1.

As a consequence, an attacker cannot produce signatures without having β_i, β_r, and s1. For authentication and validation, the signature σ_p is checked by the RSU. Hence, the attacker cannot forge it since it is generated by the proxy vehicle's private key β_i and the RSU's private key β_r.

The RSU, by checking SIG_2 can verify the result of the batch verification that has been produced by proxy vehicles. Additionally, the tamper-proof device guarantees the integrity of $\sigma_{i.1}$, generates $\sigma_{i.2}$ with the system's secret key s1 for RSUs, hence, it is impossible for the attackers to generate $\sigma_{i.2}$ and SIG_2 due to the unforgeability of signatures.

2) Identity privacy preserving

To provide privacy of identities, The pseudo-identity PS_{v_i}= ($PS_{v_i.1}$, $PS_{v_i.2}$) where $PS_{v_i.1}$= xi P, $PS_{v_i.2}$= IDi $\oplus$g(xi$P_{pub.2}$) $\oplus$ g(s3) is used instead of the real identity IDi. These are generated by tamper-proof devices. Therefore, no one can find the real identity of the vehicle except for TA since the CDH problem is hard, and no one has access to the TA's secret keys s2 and s3.

3) Unlinkability

A vehicle and its tamper-proof device generate signatures and select two random numbers for creating $\sigma_{i.1}$, $\sigma_{i.2}$. Additionally, a random number is used in pseudo identities. Therefore, based on the two mentioned reasons, RSUs and vehicles cannot link two different messages sent by the same vehicle.

4) Traceability

Only TA can obtain the vehicle's real identity, and it can extract IDi from the pseudo-identity PS_{v_i} = ($PS_{v_i.1}$, $PS_{v_i.2}$) in which $PS_{v_i.1}$= xi P, $PS_{v_i.2}$= IDi $\oplus$ g(xi Ppub,2) $\oplus$ g(s3). With the system secret keys s2, s3, it can generate IDi= $PS_{v_i.2}$ $\oplus$g (xi Ppub. 2) $\oplus$g(s3). Therefore, TA can trace and reveal vehicles' real identities and report them.

5) Resistance to Common Attacks

In the following, the proposed protocol's security against common attacks is discussed.

- ◇ Resistance to man-in-the-middle attack: To prevent such attacks, the recipient (e.g., an RSU or a proxy vehicle) needs to ensure that a specific message is sent from a licensed vehicle.

In the concrete protocol, the signatures $\sigma_{i.1}$ and σ_p are used to indicate the identity of the message sender. An adversary should have the ability to forge the used signature if it wants to implement this attack. It is failed since the used signatures are unforgeable.

◇ Resistance to impersonation attack: Each message includes a signature that identifies the sender. The adversary has to forge signatures $\sigma_{i.1}$ and $\sigma_{i.2}$ if it wants to impersonate a legitimate vehicle. Additionally, it needs to forge signature σ_p if it wants to impersonate a valid proxy vehicle. Therefore, it cannot be successful since it is assumed that signatures are unforgeable.

◇ Resistance to the replay attack: To protect the network against this type of attack, timestamps ti and tp are used to guarantee messages' freshness.

VI. COMPARISON

In this section, the presented framework is evaluated and compared to ID-MAP [28] and PBAS [25] protocols in costs and overhead features. The simulation-based comparison will then be presented (all in all, the comparisons show the presented protocol is not the best one among all, but it should be said that comparisons assume the key revocation process's cost and overhead that others do not support).

A. Computational Costs

The comparison of the proposed protocol and the two ID-MAP [28] and PBAS [25] protocols in terms of computational costs on RSU sides and in a proxy vehicle for proxy-based protocols is shortened in Table 4. In Table 4, Tmtp, Tmul, and Tp specify the required time for calculating a map-to-point function, scale multiplication operation, and pairing operation.

It is supposed that each proxy vehicle can verify the maximum of n messages. The number of verified messages in a period is d. Therefore, the number of vehicles is shown as $[\frac{d}{n}]$.

Based on the experimental results, for employing MIRACLE (Multiprocessor Integer and Rational Arithmetic C/C+ + Library) cryptographic library [30] by selecting the Tate pairing on the 160-bit subgroup of an MNT curve [31] with an embedded degree of 6 for the security level of 280, running on Intel i7 3.07 GHz machine, Tmtp, Tmul and Tp take 0. 09 ms, 0. 39ms and 3. 21ms. other operations' computational costs are very small [28]. In addition, it is assumed n= 300.

To verify 3000 signatures, the time required on RSU sides $8[\frac{d}{n}]$Tmul= $8\,[\frac{3000}{300}] \times 39\ 0/39 = 31/2$ms, in the ID-MAP[28] $5[\frac{d}{n}]$Tmul= $5[\frac{3000}{300}] \times 0/39 = 19/5$ms and in the PBAS [25] it is approximately $2[\frac{d}{n}]$Tmul + $(2[\frac{d}{n}]+ 3)$ Tp + Tmtp = $2[\frac{3000}{300}] \times 0/39 + (2[\frac{3000}{300}] + 3) \times 3/21 + 0/09 = 81/72$ms. Therefore, the proposed protocol and the ID-MAP [28] are much more practical than

Table 4. Comparison of computational costs

Protocols	Computational cost of a proxy vehicle	Computational cost of an RSU
ID-MAP [28]	(n+ 6) Tmul	$5[\frac{d}{n}]$ Tmul
PBAS [25]	d (4Tmul+ 5Tp+ Tmtp)	$2[\frac{d}{n}]$Tmul+ $(2[\frac{d}{n}]$+ 3) Tp+ Tmtp
Our protocol	(n+ 8) Tmul	$8[\frac{d}{n}]$Tmul

the PBAS [25] protocol. Moreover, the proposed protocol is more efficient due to revocation [28].

The required time of the proxy vehicle in the proposed protocol is (n+ 8) Tmul= (300+ 8) × 0/39= 120/12ms, while in ID-MAP [28] is (n+ 6) Tmul= (300+ 6) ×0/39= 119/5ms and in PBAS [25] is n(4Tmul+ 5Tp+ Tmtp)= 300 (4 × 0/39+ 5 × 3/21+ 0/09)= 5310ms. As a result, the proposed protocol has a better performance at revocation, and it is not so different from the protocol of ID-MAP [28].

B. Communication Overhead

In this section, we are planning to show the comparison of communication overhead related to our proposed protocol with ID-MAP [28] and PBAS [25] protocols in terms of transmitting d messages to an RSU is shown in Table 5. For the security level 280, it is assumed that q= 160 bits and each element is G be 40 bytes. In addition, the time stamp size is assumed 4 bytes (it should be noted that the size of message mi is not considered since it is unique in all authentication protocols). In PBAS [25], the sent message from a vehicle to the proxy vehicle is {$PS_{v_i.1}$, $PS_{v_i.2}$, Ti, σi,1, σi,2} where σi,2, σi,1, $PS_{v_i.1}$ and $PS_{v_i.2}$∈ G, so we have 40×4+ 4= 164 bytes, and to send d messages we have 164d. The message sent by a vehicle to a proxy vehicle in ID-MAP [28] is {$PS_{v_i.1}$, $PS_{v_i.2}$, Ti, Wi, σi,1, σi,2}, where $PS_{v_i.1}$, $PS_{v_i.2}$ and Wi ∈ G, σi,2 and σi,1 ∈ Z_q^*, so communication cost is calculated as 40 × 4+ 2 × 20+ 4= 204 bytes, and for sending d messages its value is 204d, while in the proposed protocol the message send by a vehicle to a proxy vehicle is {$PS_{v_i.1}$, $PS_{v_i.2}$, ti, mi, Ri, Zi, W, RKi, $\sigma_{i.1}$, $\sigma_{i.2}$} where, $PS_{v_i.1}$, $PS_{v_i.2}$, RKi, Ri, Zi and Wi ∈ G and σi,2, σi,1 ∈ Z_q^*. Hence, the communication overhead in the proposed protocol for sending d messages is calculated as (6×40+ 2×20+ 4) d= 284d bytes.

Imagine each proxy vehicle verifies n messages, so the number of proxy vehicles to verify d messages is assumed as $[\frac{d}{n}]$. In PBAS [25], the sent messages by a proxy vehicle to an RSU is {$PS_{v_p,1}$, $PS_{v_p,2}$, Tp, σp, σ1, σ2, $PS_{v_i.1}$, $PS_{v_i.2}$, Ti, 1≤ i ≤ d} where $PS_{v_p,1}$, $PS_{v_p,2}$, $PS_{v_i.1}$, $PS_{v_i.2}$, σp, σ1 and σ2 ∈ G. So the communication overhead by $[\frac{d}{n}]$ number of proxy vehicles is calculated as (40×5+ 4) $[\frac{d}{n}]$+ (2×40+ 4) d= 204$[\frac{d}{n}]$+ 84d bytes, and the message sent by a proxy vehicle to the RSU in ID-MAP [28] is {$PS_{v_p,1}$, $PS_{v_p,2}$, Tp, Rp, σp, σ1, σ2, $PS_{v_i.1}$, $PS_{v_i.2}$, Wi, Ti,

1≤ i ≤d}, where $PS_{v_p,1}$, $PS_{v_p,2}$, $PS_{v_i.1}$, $PS_{v_i.2}$, Wi and Rp ∈ G. Therefore, the communication overhead is calculated as (40×3+ 3×20+ 4) $[\frac{d}{n}]$+ (3×40+ 4) d= 184 $[\frac{d}{n}]$+ 124d bytes. Additionally, the sent message by a proxy vehicle to the RSU in the proposed protocol is {$PS_{v_i.1}$, $PS_{v_i.2}$, Ri, ti, σ1, σ2, $PS_{v_p,1}$, $PS_{v_p,2}$, Zp, σp, Tp, RKp, 1≤ i ≤d} where $PS_{v_p,1}$, $PS_{v_p,2}$, $PS_{v_i.1}$, $PS_{v_i.2}$, Ri,RKp and Zp ∈G, σ1, σ2 and σp ∈ Z_q^*. Therefore, the communication overhead of the proposed protocol is calculated as (4 × 40+ 3 × 20+ 4) $[\frac{d}{n}]$+ (3 × 40+ 4) d= 224 $[\frac{d}{n}]$+ 124n bytes. In proxy-oriented protocols, it is assumed that n= 300 [25, 28].

To send 3000 signatures to the RSU, the size of the message sent in PBAS [25] is 204$[\frac{3000}{300}]$ + 84×3000= 254040 bytes and in ID-MAP is 184 $[\frac{3000}{300}]$+ 124 × 3000= 373840 bytes, while this value in the proposed protocol is 244 $[\frac{3000}{300}]$+ 124 × 3000= 374440 bytes; And the size of the sent message to a proxy vehicle by vehicles in PBAS [25] and ID-MAP [28] protocols are 164 × 300= 49200 bytes and 204 × 300= 61200 bytes, respectively, while in the proposed protocol this value is 284 × 300= 85200 bytes. However, this issue does not affect the VANETs' efficiency since vehicles approach the proxy vehicles and communicate directly with them, so communication overhead is distributed among them. As a result, our scheme reduces communication overhead at RSUs. As shown in Table 5, the proposed protocol, despite the use of revocation operations, is similar to Asaar et al. 's protocol [28]. However, the communication overhead of our scheme and ID-MAP [28] compared to that of PBAS [25] is increased. As a consequence, the performance of the proposal scheme is not better than the performance of ID-MAP but it supports managing the revocation list. Our enhanced scheme also has a more acceptable communication overhead on the RSU side.

C. Simulation-based Comparison

The proposed protocol is simulated in NS2-35, which is flexible and provides an environment to compare existing protocols, and VanetMobiSim [32] is used to simulate the mobility model of a vehicle. The outcomes show the average message delay and the average loss ratio in RSUs for analyzing the proposed protocol's performance and comparing it with ID-MAP [28] and PBAS [25] protocols (it should be noted that in the first two simulation results, the vehicle speed is about 10 ~30 m/s, and the number of vehicles in the last two simulation results is assumed 100). The parameters and scenario of the road can be seen in the mobility model used by Liu et al. [25] are given in Table 6.

Fig. 2 compares the Average Message Delay (AMD), which indicates the time required to transfer messages from a vehicle to the RSU of the proposed protocol versus the number of vehicles in ID-MAP [28] and PBAS [25] protocols. As shown in Fig. 2, all protocols' AMD is

Table 5. Comparison of communication overheads (in bytes)

Protocols	Sending d messages to a proxy vehicle	Sending d messages to an RSU
ID-MAP [28]	204d	$184[\frac{d}{n}]+124d$
PBAS [25]	164d	$204[\frac{d}{n}]+84d$
Our protocol	284d	$224[\frac{d}{n}]+124n$

Table 6. Simulation parameters [25]

Parameters	Values
Coverage area	8000×16m2
No. of traffic lanes	4
No. of RSUs	5
Maximum No. of proxy vehicles	20
Simulation duration	100s
MAC layer protocol	802. 11p
Channel bandwidth	6 Mbps
Transmission range of a vehicle	300 m
Transmission range of an RSU	1000 m
Minimum inter-vehicle distance	40 m
Routing protocol	AODV
Slot time	13μs
SIFS	32μs
AIFS (high priority)	58μs
Contention window size (CW)	15 ~ 1023μs

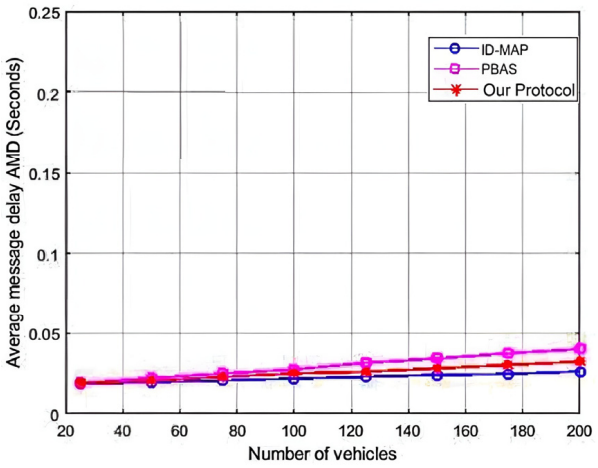

Fig. 2. Average message delays versus vehicles' number in RSUs

increased gradually as proxy vehicles reduce the number of handshakes between vehicles and RSUs considering the vehicle's number. Additionally, the compared protocols' AMD has been increased compared to ID-MAP [28] since the proposed protocol's computation overhead is increased.

Fig. 3 shows the Average Message Loss Ratio (AMLR) versus vehicle's number. Which is the ratio between the number of dropped messages and the total number of messages received by an RSU in each 100s, in the proposed protocol, ID-MAP [28] and IPBAS [25] protocols versus the number of vehicles. Since Ad hoc On-Demand Distance Vector (AODV) protocol which uses relays for routing, is used to simulate protocols, it helps vehicles with the transmission range of 300 m in forwarding messages as the relay increases, AMLR all protocols are reduced. However, the AMLR protocols increase due to the collision caused by the hidden terminal problem and the frequent transfer between RSUs and vehicles in the same communication area with 100 vehicles. The ID-MAP has the bottommost AMLR compared to the other two schemes, but the proposed scheme is worthwhile since it supports revocation. As a result, the time of direct transfer between vehicles and RSUs is reduced by using proxy vehicles.

Fig. 4 compares AMD of the proposed protocol and ID-MAP [28] and PBAS [25] protocols regarding average vehicles' speed. As shown in Fig. 4, AMD is almost constant for different values of speed. On the one hand, with the increase in the number of vehicles, AMD of all schemes increases, and on the other hand, more packages will be dropped with an increase in the average speed of vehicles. Therefore, these two events effectively cancel the effect of each other. As a result, simulation results show that the AMD of all protocols has been slightly affected by the increase in the vehicle's speed. However, the AMD of the proposed scheme because of having more operation due to providing revocation is more than that of ID-MAP [28], and also it has a lower AMD compared to PBAS [25] because of faster verification of messages by RSUs.

Fig. 5 shows a comparison of AMLR of the proposed protocol and the two ID-MAP [28] and PBAS [25] protocols in terms of the vehicles' average speed. However, increasing the average vehicle speed incredibly affects the AMLR of schemes since transmission is cut off as vehicles run quickly. ID-MAP [28] has the bottommost AMLR levels than others since the assumed proxy vehicles reduce direct transmission on vehicles and RSUs. However, due to more operations to satisfy revocation, the proposed protocol has a higher AMLR than ID-MAP [28].

VII. CONCLUSION

This study presented an efficient framework developed for the message verification at roadside units with proxy vehicles in VANETs. The presented framework used "online" and "offline" signatures for the message generation. Also, in the proposed protocol, vehicles using the network have revocation keys. After receiving sufficient protest messages from other vehicles, the trusted authority revokes malicious vehicles, and RSUs are responsible for managing revocation lists of its coverage area. The new authentication protocols met security requirements such as message

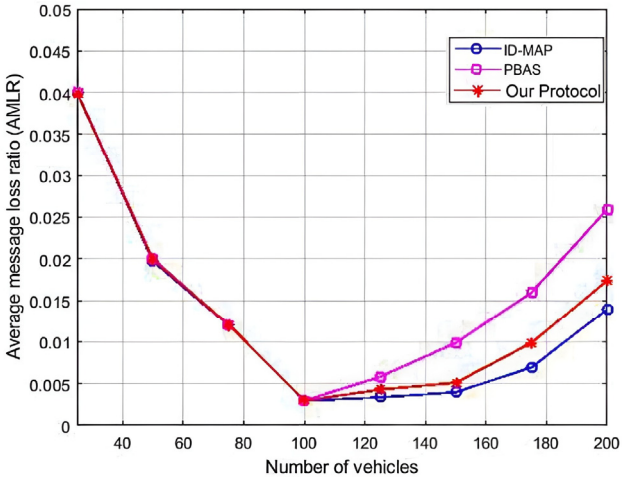

Fig. 3. Average message loss ratios versus vehicles' number in RSUs

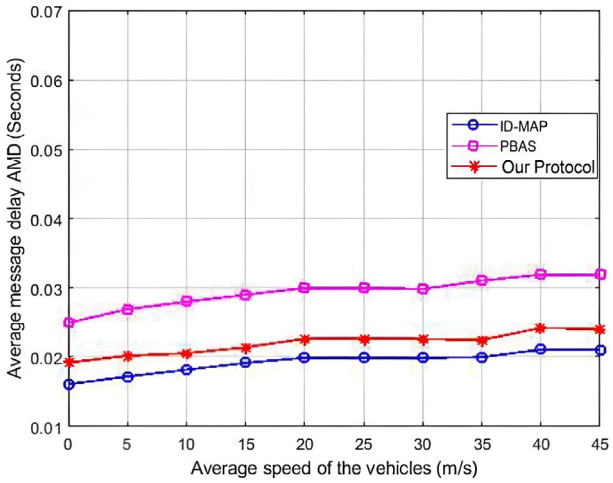

Fig. 4. Average message delays versus vehicles' speed in RSUs

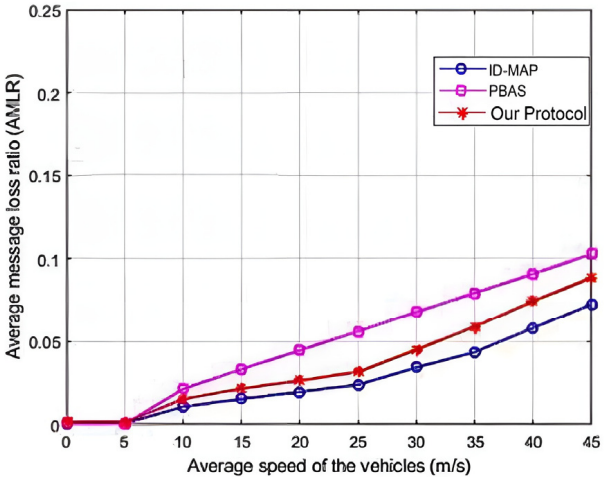

Fig. 5. Average message loss ratios versus vehicles' speed in RSUs

authentication, unlinkability, privacy-preserving, traceability, and resistance to attacks such as a man in the middle, impersonation attack, and reply attack. Outcomes, analysis, and comparison of computational and communication overhead showed the proposed protocol's efficiency and practicality.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers and editors for their valuable remarks and suggestions on the content of this paper.

REFERENCES

[1] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, pp. 217-241, Aug. 2012.

[2] F. Li and Y. Wang. "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology magazine,* vol. 2, no. 2, pp. 12-22, June 2007.

[3] Z. Shi, B. Cory, and K. Mitchell, "Analytical models for understanding space, back off, and flow correlation in CSMA wireless networks," *Wireless networks*, vol. 19, no. 3, pp. 393-400, 2013.

[4] M. Raya and J. Pierre, "Securing vehicular ad hoc networks," *Jour. Comput. Secur.,* vol. 15, no. 1, pp. 39–68, 2007.

[5] J. Shen, Z. Tianqi, W. Fushan, S. Xingming, and X. Yang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," *IEEE Internet of Things Journal, vol. 5*, no. 4, pp. 2526-2536, 2017.

[6] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: prediction-based authentication for vehicle-to-vehicle communications," *IEEE Trans. Dependable and Secure Computing*, vol. 13, no. 1, pp. 71–83, Jan.-Feb 2016.

[7] A. Studer, F. Bai, B. Bellur, et al., "Flexible, extensible, and efficient VANET authentication," *J. Commun. Netw*., vol. 11, no. 6, pp. 574– 588, 2009.

[8] A. Perrig, C. Ran, J. Doug Tygar, and S. Dawn, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes,* vol. 5, no. 2, pp. 2-13, 2002.

[9] IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE), U. S. Dept. Transportation, 2009.

[10] N. -W. Wang, Y. -M. Huang, and W. -M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer Communications*, vol. 31, pp. 2827–2837, 2008.

[11] R. Lu, X. Lin, H. Zhu, et al., "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *in Proc. IEEE INFOCOM*, pp. 1229–1237, March 2008.

[12] Y. Sun, R. Lu, X. Lin, et al., "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," *IEEE Trans. Veh. Technol*., vol. 59, no. 7, pp. 3589–3603, Sept. 2010.

[13] A. Wasef and S. Xuemin, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. *12*, no. 1, pp. 78-89, Jan. 2013.

[14] H. Lu, J. Li, M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," *In IEEE Computing, Communications and Applications Conference (ComComAp)*, 2012, pp. 345-350., Feb. 2012.

[15] C. Zhang, R. Lu, X. Lin, P. -H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," *in Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM'08)*, pp. 246– 250, Phoenix, Ariz, USA, April 2008.

[16] T. W. Chim, S. -M. Yiu, L. C. K Hui, V. O. K. Li," SPECS: Secure and privacy-enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189-203, 2011.

[17] K. -A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Vehicular Technology*, vol. 61, no. 4, pp. 1874– 1883, May 2012.

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

[19] J. Zhang, M. Xu, L. Liu, "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

[20] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[21] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs*," IEEE Trans. Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516– 526, March 2017.

[22] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, April 2015.

[23] S. Even, O. Goldreichmm, and S. Micali, "On-line/off-line digital signatures," *In Conference on the Theory and Application of Cryptology*, pp. 263-275. Springer, New York, NY, 1989

[24] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[25] Y. Liu, L. Wang, and H. -H. Chen, "Message authentication using proxy vehicles in vehicular as hoc networks," *IEEE Trans. Vehicular Technology*, vol. 64, no. 8, pp. 3697-3710, Aug. 2015.

[26] A. Malhi and S. Batra, "Privacy-preserving authentication framework using bloom filter for secure vehicular communications," *International Journal of Information Security*, vol. 15, no. 4, pp. 433-. 453, 2016.

[27] Y. Xie, L. Wu, J. Shen, A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," *Telecommunication Systems*, vol. 65, no. 2, pp. 229-240, 2017.

[28] M. Rajabzadeh Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi," A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks*," IEEE Trans. Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, June 2018

[29] R. Barskar and M. Chawla, "Vehicular ad hoc networks and their applications in diversified fields," *International Journal of Computer Applications,* vol. 1, no. 10, Jan. 2015.

[30] MIRACL Cryptographic Library: Multiprecision Integer and Rational Arithmetic C/C+ + Library. Available: http:// indigo. ie /

[31] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundamentals*, vol. E84-A, no. 5, pp. 1234–1243, 2001.

[32] VanetMobiSim Project Home Page. Available: http://vanet. eurecom. fr.

[33] C. Zhang, X. Xiaoping, F. Lijuan, Z. Xin, and M. Jingxiao, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access,* vol. 7, pp. 178310-178320, 2019.

[34] J. Shen, L. Dengzhi, C. Xiaofeng, L. Jin, K. Neeraj, and V. Pandi," Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Trans. Vehicular Technology,* vol. *69*, no. 1, pp. 807-817, 2019.

[35] X. Li, H. Yue, G. Juntao, and N. Jie, "Secure hierarchical authentication protocol in VANET," *IET Information Security,* vol. *14*, no. 1, pp. 99-110, Jan. 2019.

[36] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal,* vol. 14, no. 3, pp. 3547-3557, Sept. 2020.

[37] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan. "Efficient lattice-based ring signature for message authentication in VANETs." *IEEE Systems Journal,* vol. 14, no. 4, pp. 5463-5474, Dec. 2020.

[38] P. Wang and L. Yining, "SEMA: Secure and Efficient Message Authentication Protocol for VANETs." *IEEE Systems Journal,* vol. 15, no. 1, pp. 846-855, 2021.

[39] K. Mahmood, A. Rehman, P. Chaudhary, X. Li, F. Wu, and S. Kumari, "Revised anonymous authentication protocol for adaptive client-server infrastructure," *International Journal of Communication Systems*, vol. 33, no. 4, e4253, March.2020.

[40] P. Bhuarya, P. Chandrakar, R. Ali, and A. Sharaff, "An enhanced authentication scheme for the Internet of Things and cloud-based on elliptic curve cryptography," *International Journal of Communication Systems,* vol. 34, no. 10, e4834, July 2021.

[41] M. Javad Sadri and M. Rajabzadeh Asaar, "An efficient hash-based authentication protocol for wireless sensor networks in Internet of Things applications with forward secrecy," *International Journal of Communication Systems*. vol. 10, no. 34, e4823, July 2021.

[42] G. Baskaran, S.K. Kannaiah, and S. Ramanujam, "A secured authentication and DSM□KL ascertained performance optimization of a hybrid blockchain-enabled framework for a multiple WSN," *International Journal of Communication Systems,* vol. 24, no. 34, e4972, Nov. 2021.

[43] V. S. Naresh, S. Reddi, and V.D. Allavarpu, "Lightweight secure communication system based on Message Queuing Transport Telemetry protocol for e-healthcare environments," *International Journal of Communication Systems*, vol. 34, no. 11, e4842, July 2021.

[44] S. Jiang, H. Cheng, and Y. Liu, "LPTM: Lightweight and privacy-preserving traffic monitoring scheme," *International Journal of Communication Systems,* vol. 35, no. 13, e5245, Sept. 2022

[45] J. N. Hwang, "Wireless MediaNets: application-driven next-generation wireless IP networks. Multimedia Systems. vol. 17, pp. 251–285, 2011.

[46] P. Derakhshan-Barjoei, G. Dadashzadeh, F. Razzazi, S.M. Razavizadeh, "Power and time slot allocation in cognitive relay networks using particle swarm optimization," *The Scientific World Journal*, vol. 2013, Article ID 424162, 9 pages, 2013.

[47] P. Derakhshan-Barjoei, G. Dadashzadeh, F. Razzazi, S.M. Razavizadeh, "Bio-inspired distributed beamforming for cognitive radio networks in non-stationary environment," *IEICE Electronics Express,* vol. 8, no. 6, pp. 332-339, 2011.