Efficient Privacy Preserving Anonymous Authentication Announcement Protocol for Secure Vehicular Cloud Network

Nur Afiqah Suzelan Amir[1], Wan Ainun Mior Othman[1*], and Kok Bin Wong[1]
[1] Institute of Mathematical Sciences, Faculty of Science, University of Malaya
50603, Kuala Lumpur, Malaysia.
[e-mail: nurafiqah@um.edu.my, wanainun@um.edu.my, kbwong@um.edu.my]
[*]Corresponding author: Wan Ainun Mior Othman

Received August 29, 2022; revised April 10, 2023; accepted May 8, 2023; published May 31, 2023

Abstract

In a Vehicular Cloud (VC) network, an announcement protocol plays a critical role in promoting safety and efficiency by enabling vehicles to disseminate safety-related messages. The reliability of message exchange is essential for improving traffic safety and road conditions. However, verifying the message authenticity could lead to the potential compromise of vehicle privacy, presenting a significant security challenge in the VC network. In contrast, if any misbehavior occurs, the accountable vehicle must be identifiable and removed from the network to ensure public safety. Addressing this conflict between message reliability and privacy requires a secure protocol that satisfies accountability properties while preserving user privacy. This paper presents a novel announcement protocol for secure communication in VC networks that utilizes group signature to achieve seemingly contradictory goals of reliability, privacy, and accountability. We have developed the first comprehensive announcement protocol for VC using group signature, which has been shown to improve the performance efficiency and feasibility of the VC network through performance analysis and simulation results.

Keywords: Reliability, Privacy, Accountability, Announcement, Vehicular Cloud, Group Signature.

1. Introduction

According to the US Department of Transportation (US-DOT), multiple cases of traffic congestion have led to a loss of productivity worth over 75 billion dollars for workers and wastage of more than 8.4 billion gallons of gasoline over the past few years [1]. This has led to a growing interest in the development of secure vehicular communications in the past decade. To address this, researchers have focused on the construction of vehicular ad hoc networks (VANETs) to enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications that can improve road safety and traffic efficiency [2-6]. However, VANETs have limited capacity to process, analyze, and evaluate the vast amounts of data generated by vehicles and infrastructure for emerging advanced vehicle technologies [7-8]. Therefore, there has been a proposed shift from traditional VANETs to vehicular cloud (VC) networks.

The concept of vehicular cloud has been evolving with two main paradigms: Vehicular Ad Hoc Network (VANETs) and cloud computing (CC). Cloud computing is a model of distributed computing that provides a range of services to users over the internet, including computing resources, storage, applications, servers, and networks. This technology has attracted a lot of attention from various entities such as governments, research institutes, and industry leaders [2, 10-17]. It has the potential to resolve the computing and storage issues that arise on the internet. The integration of cloud computing with VANETs can enhance road safety and traveling experience. By adopting CC, the computation burden of verifying safety messages on the receiving vehicle can be reduced, as CC offers services on demand to users.

Security and privacy concerns have been a major focus in the development of VC, and several studies have proposed the integration of VANET with cloud computing (CC) [18-25]. Olariu et al. [22] suggested the concept of VC, which refers to a collection of vehicles that collaborate by pooling their computing, sensing, communication, and physical resources that can be assigned to authorized vehicles in a dynamic manner. Similarly, Yan et al. [25] conceptualized VC as the dynamic combination of resources and information while vehicles are in motion.

Announcement protocols in VC broadcast a warning message to nearby vehicles in the network to alert them of a potential safety hazard, such as an accident or road blockage. This ensures that the message is delivered to all nearby vehicles in a timely and reliable manner, and that the authenticity and integrity of the message is verified to prevent any malicious attacks. To utilize the advanced features of VC, safety messages should be delivered in a way that reflects the actual situation while maintaining privacy. Nevertheless, ensuring the reliability of the message may reveal the identity of the sender.

A safety message can be considered trustworthy if it originates from a legitimate vehicle and has not been tampered by any unauthorized adversary. [15]. In VANET it is generally presumed that there are adversaries within the network [2, 3, 5, 26–27]. Adversaries might be insider or outsider. An entity that lacks legitimate access and credentials to engage in the network system is referred to as an outsider. Meanwhile, a legitimate user with current credentials issued by a trusted party (TP) in the network is an insider. An insider may misuse their legitimacy thus impose more harm to other vehicles in the network. We consider the presence of insider in our work.

There are several protocols that address the issues of message reliability, privacy, and accountability in VC networks. A safety message is **reliable** if and only if satisfy the three requirements:

- The authentic vehicles possess valid credentials issued by a TP (sender's authenticity).
- The safety message is secured against illegal alteration (message integrity) [44].

- The evaluation of reliability of the safety message (message truthfulness) [2, 5].

The two features of **privacy,** which are anonymity and unlinkability. Anonymity means that identity of a sender must be protected. When two communications are unlinkable, it signifies that it is impossible to distinguish whether they originate from the same vehicle or not. The **accountability** requirement must be satisfied to make the network robust and vulnerable against attacks [39]. The misbehaving vehicle may be tracked by the TP in the event of a dispute, and it cannot deny having issued a message. The misbehaving vehicle will be revoked from continuing participation in the network if proven to have misbehaved.

To address the first two requirements of message reliability, digital signature technique is commonly used [18-20, 24, 38, 40, 42-43, 46-47]. Nevertheless, validating the reliability of the message may permit irresponsible entities to track and monitor vehicles for the purpose of profiling. To achieve last requirement of message reliability, one of the techniques is via threshold method. The threshold method is widely adopted in announcement protocols in VANET [2,27,41,44]. In a threshold technique, an announced message is reliable if it was reported by several reputable sender of a particular threshold. The threshold technique, on the other hand, requires a distinguishable message origin so that a verifier may check if the same sender provides two distinct signatures on the same message. However, this is conflicting with privacy. A lack of privacy enables profiling by an adversary which leads to the disclosure of sensitive data. Thus, preserving a privacy of the sender is necessary in a VC network.

To enforce accountability, the VC network must be able to trace the misbehaved vehicle so that a vehicle could not deny as the message originator. However, it contradicts the privacy requirement by opening the signature. The property of revocability is desirable in certain applications. Resolving security conflicts between reliability, privacy and accountability is essential for a secure and efficient announcement protocol in VC network. To address this challenge, we introduce a new announcement protocol for VC that builds upon and extends an existing scheme of [27]. We leverage the latest advancements in VC technology and offer additional benefits such as ease of use, accessibility, and reduced deployment costs [37]. Our protocol is designed with the following desirable features:

- We develop a generic abstraction of a group signature announcement protocol. This generic abstraction intends to serve as a framework for the development of announcement protocols in the future that employ group signature in VC. According to our knowledge, this is the first construction of such an abstraction for VC that has been introduced in the literature.
- We analyse the advantages and disadvantages of the existing literatures, scrutinize the cryptographic primitive adopted in previous work and discuss the elements of security required for a secure deployment of announcement protocol in VC. We then present and propose the first systematic design of an announcement protocol of VC using group signatures and deals with the competing security demands of message reliability, privacy, and accountability simultaneously.
- We provide an analysis and simulation results that demonstrate the practical security level, system robustness, and performance efficiency of our protocol, which can be effectively applied and scaled in real-world implementations.

The structure of the paper is as follows. In Section 2, we discuss the advantages and limitations of current vehicular cloud (VC) schemes, as well as relevant research related to announcement protocols in VC. Section 3 describes the generic announcement construction. Section 4 provides an overview of the WDG scheme that we extend and modify in our work.

In Section 5, we introduce and present the proposed announcement protocol. We evaluate the performance and security of our protocol in Section 6. We conclude the paper in Section 7 and provide recommendations for future research directions.

2. Related Work

A number of literatures [18-20, 24, 38, 40, 42-43, 46-47] uses the location-based encryption for announcement protocol in VC network. In these proposed schemes, the reliability of a message is assured by merging geographic and time into conventional encryption algorithm. In [42], the reliability of a message is assured by merging geographic and time into a conventional encryption algorithm. Physical location encryption can provide a way to secure communication by limiting the ability to decrypt the cipher text to a specific geographical area. This method improves security by preventing decryption of the message at any location outside of the specified area, resulting in decryption failure. Therefore, the announcement message would not be broadcasted and utilized. In addition, the issue of privacy and accountability was not addressed in their work.

Yan et al. [24, 38] developed a technique for location-based encryption called Geoencrypt, which builds on prior work [42] and utilizes a symmetric algorithm. This technique uses a vehicle's geographic location to generate a private key that is distributed by the trusted party (TP) to sign messages, thereby fulfilling the first two requirements for message reliability. However, Geoencrypt is not suitable for a threshold mechanism where message origin distinguishability cannot be achieved. To maintain anonymity, the technique employs a pseudonym-changing-based authentication method that regularly changes and updates pseudonyms to keep the identity of the signer hidden. The scheme requires the use of each pseudonym only once or for a limited time based on the desired level of privacy. However, a drawback of this approach is that it necessitates frequent communication between the TP and the vehicles to establish symmetric key authentication each time a vehicle signs a message.

Hussain et al. [18-20] proposed a VANET-based cloud framework called VANET using clouds (VuC) as an improvement over [38]. They introduced geolock encryption, which generates keys based on location information to ensure message authentication through legitimate vehicles with valid credentials from the TP. For privacy, they used identityless beacon messages called Mobility Vectors (MVs) that do not contain any identifiable information linking the sender to the message. However, this approach does not allow for distinguishing the origin of the message, so the threshold mechanism cannot be applied. To achieve accountability, the authors utilized traditional certificate revocation lists (CRLs) to distribute certificate revocation information across the network.

An enhanced identity-based authentication protocol for VC was proposed by Balamesh et al. [40] to improve the efficiency of location-based services while preserving the privacy of a vehicle. It presents anonymous authentication to vehicles and provides dual registration detection. A vehicle adopts pseudo-ID to protect its true identity during a service session. The session key is being kept at different time slots of the service sessions. On the other hand, the involvement of roadside units (RSU) is needed in this scheme to update the session key. From their analysis, they claimed that RSU generate short-time anonymous certificate to each vehicle thus essentially preserve the message linkability. Nonetheless, to authenticate the credential using this approach, frequent communication with the TP is necessary, however the TP might not always be accessible.

Nkenyereye et al. [43] proposed a new security protocol for securing traffic management in VC based on identity-based authentication which is the extension of [18-20]. To create a

signature on a message, a tamper proof device (TPD) produces pseudo-identities for each vehicle. Message authentication is satisfied in this case. Due to the indistinguishability of the message's origin, threshold adaptive authentication cannot be used. Various pseudonyms are used to sign communications to ensure anonymity and unlinkability. However, the TP must be entirely trusted because it possesses the private keys to the respective vehicle.

Zhang et al. [46] proposed a dynamic identity-based asymmetric group key agreement scheme for vehicular networks, which involves a one-time pseudonym connected with a vehicle's actual identity. The private key related to the pseudonym, distributed by a trusted party (TP), functions as the vehicle's credential for signing safety messages. The usage of valid credentials from a TP for message signing guarantees message authentication. TP maintains a database for all registered vehicles in the network and can retrieve a vehicle's actual identity if it engages in malicious behavior. The pseudonym guarantees anonymity for the sender, but it cannot differentiate between two messages signed by the same vehicle, making a threshold method implementation unfeasible. Additionally, the scheme suffers from a key escrow problem.

Li et al. [47] proposed a VC security scheme that combines identity-based security and blockchain technology. Under this scheme, each vehicle is assigned a unique identity and uses a group encryption key to sign messages, which provides message authentication. However, the scheme cannot differentiate between messages signed by the same vehicle, making threshold mechanism unfeasible. Short-term anonymous credentials generated by RSU ensure privacy, and TP generates private keys for public keys to enable traceability. However, the paper did not discuss revocability. Additionally, the use of blockchain technology may lead to high communication costs and inefficiencies when there are many vehicles in the network.

Location based encryption requires a receiving vehicle to be physically present to be able to decrypt the message, otherwise message announced would not be utilized. In an announcement scheme, location of an event reported should not be kept private to any receiving vehicle as safety-related messages are often associated to an event of a location in the vicinity of the event reported. This contradicts to the nature of an announcement scheme. The VC schemes in [18-20, 24, 38, 40, 42-43, 46-47] satisfies the requirement of user authentication and message integrity. However, there is no means to evaluate message reliability in all the VC schemes proposed. Thus, threshold method cannot be utilized. In terms of privacy, these VC schemes achieve anonymity and unlikability. The responsibility of accountability is placed on the TP, who is considered a completely reliable entity, and has access to the secret key of the vehicle. Consequently, the concept of non-repudiation is not fulfilled in [18-20, 24, 38, 40, 42-43, 46-47], since the vehicle is not the only one with access to the signing key. Furthermore, matter of revocability was also not addressed in [18-20, 24, 38, 40, 42-43, 46-47].

3. Generic Announcement Construction

3.1 System Structure

The network architecture comprises a cloud-based trusted party (C_{TP}), roadside units (RSUs), and vehicles consisting of a sending vehicle (Vs) and a receiving vehicle (Vr). The responsibilities of each entity are outlined below:

1) **Cloud (C_{TP})**. We utilize a cloud network as a trusted third party (TP) for managing vehicle access and revocation of dishonest vehicles. The cloud is responsible for issuing and

managing credentials, as well as detecting and identifying misbehaving vehicles. The cloud is also responsible for verifying the trustworthiness of safety messages, which can help reduce the computational burden for the receiving vehicle (Vr).

2) **Road Side Unit.** The road side unit (RSU) is a physical infrastructure situated at the side of the road, distributed extensively in metropolitan areas due to high population density. RSUs play a limited role in our protocol, serving as intermediaries for relaying information between vehicles and the cloud via short-range communication. Prior to joining the network, the cloud authenticates and verifies each RSU.

3) **Vehicle**. In a VC network, there are two types of vehicles, namely sending vehicles (Vs) and receiving vehicles (Vr). Safety-related messages are generated and forwarded by Vs, while Vr utilizes and responds appropriately to the received safety-related messages.

In our network, we assume that every vehicle has an onboard unit (OBU) which is a computing device. The OBU's wireless communication capability includes an Event Data Recorder (EDR) that records received messages. Additionally, the OBU has a Trusted Platform Module (TPM) as a built-in component that employs cryptographic tools and manages access control.

3.2 Generic Abstraction

We formulate a generic abstraction for a group signature announcement protocol in VC. The different stages of the outline are depicted in **Fig. 1** and can be summarized as follows:

Registration Phase

Step 1: V_s sends a request to obtain a credential from the C_{TP} in order to join the network.
Step 2: C_{TP} produces, issues, and stores credentials to verify V_s authenticity in the network.
Step 3: The C_{TP} provides the credential to V_s upon successful authentication.

Transmission Phase

Step 4: By using RSU, V_s generates and broadcasts a safety message related to the incident to the C_{TP}.
Step 5: Between the C_{TP} and the Vs, RSU serves as a gateway, transmitting the safety message for authentication.

Validation Phase

Step 6: C_{TP} authenticates the reliability of a message.
Step 7: Upon successful verification, the C_{TP} will deliver the safety related announcement to a nearby RSU that associated to the event reported.
Step 8: RSU broadcast the authenticated safety message to V_r corresponding to the vicinity of event reported.
Step 9: V_r verifies the message and utilize the safety related announcement for a safer and more conducive travelling environment.

Tracking and Revoke Phase

Step 10: If V_r encountered any wrongdoing during its interaction with V_s, they may lodge a report to the C_{TP} via the nearby RSU.
Step 11: The C_{TP} evaluates the validity and reliability of the information after receiving reports before considering eliminating V_s from the network.

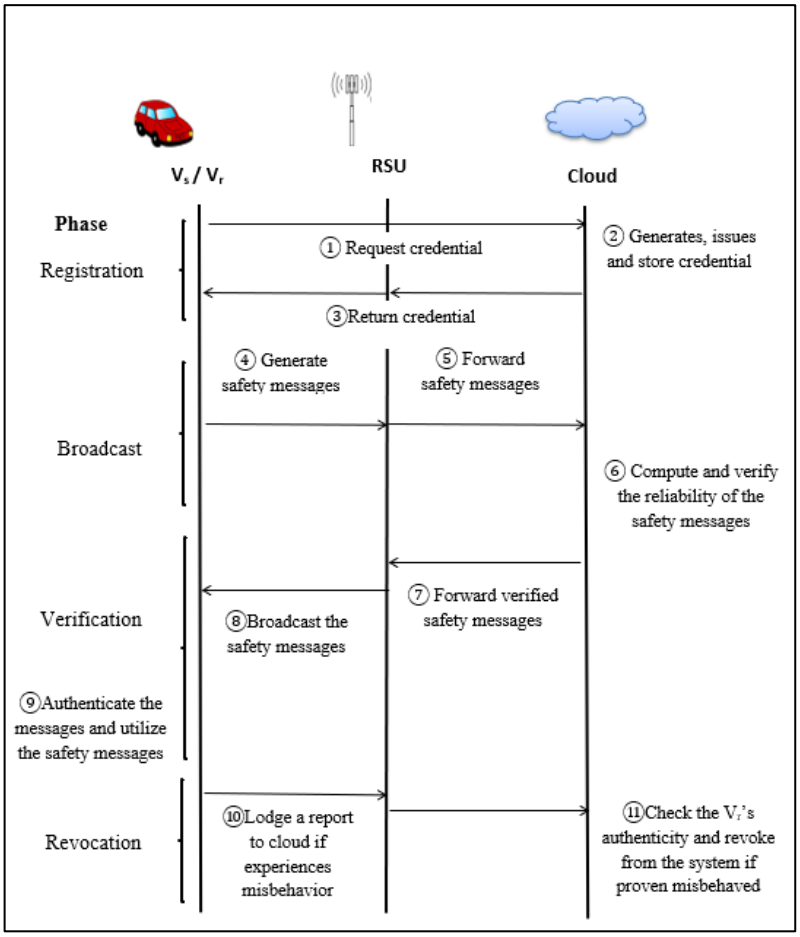

Fig. 1. Generic Abstraction.

4. The WDG Construction

Wu, Domingo-Ferrer, and Gonzalez-Nicolas (WDG) introduced a group signature scheme that allows message linkage using bilinear-pairing groups and anonymous threshold authentication. This scheme allows receivers to only accept messages that have been verified by a specific minimum number of anonymous vehicles, which prevents Sybil attacks. The scheme includes three Trusted Parties (TPs): Vehicle Manufacturers ($\mathcal{VM}$), the group registration manager ($\mathcal{RM}$), and the tracing manager ($\mathcal{TM}$). A vehicle must sign a contract with the $\mathcal{VM}$ to be registered and participate in the network. After being registered to the $\mathcal{RM}$, the vehicle can access the network and generate a public key Y= U_1^y for an arbitary value $y \in \mathbb{Z}_p^*$, which is its secret key. To ensure traceability, the tracing data $T = g_2^y$ is submitted to the $\mathcal{TM}$ during registration. The $\mathcal{VM}$, $\mathcal{RM}$, and $\mathcal{TM}$ are assumed to be trustworthy as they have no access to the vehicle's private keys. $\mathcal{RM}$ provides a signature to the vehicle's public key after successful network registration, which is used by the vehicle as a group certificate to disseminate safety messages. The objective of the WDG scheme is to achieve a balance between ensuring public safety and maintaining the privacy of the vehicles. **Table 1** shows some of the notations used in the protocol adapted from [27] for ease of reading throughout the paper.

Table 1. Table of Symbol and Notation

Notation	Description
$\mathcal{TKC}$	Tracking cloud
$\mathcal{RGC}$	Enrolment cloud
$\mathcal{ATC}$	Confirmation cloud
$\mathcal{V}$	Vehicle
$\mathbb{G}_i (i = 1,2,3)$	Finite cyclic group of prime order p
g_i	A random generator of $\mathbb{G}_i$
$U_2, h_2, U_p \in \mathbb{G}_2$	Public system parameters
$\emptyset$	An isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$
$U_1 = \phi(U_2)$	Public system parameter
$h_1 = \phi(h_2)$	Public system parameter
$H_1( )$	A cryptographic hash function from $\{0,1\}^*$ to $\mathbb{G}_1$
(A, Z)	$\mathcal{RC}$'s public-private key pair
$\mathcal{PK}_v$, $\mathcal{SK}_v$	$\mathcal{V}$'s key pair
MT	Message type
GI_v	Group identifier for the vehicle
I_{RSU}	RSU's actual identification is I_{RSU}
$K_v = (K_1, K_2)$	The group certificate of vehicle
$T_v = g_2^{\mathcal{SK}_v}$	The tracking data of vehicle
m	A message
σ	A signature on message m
$\mathcal{M} = (m, \sigma)$	A message appended with a signature
σ_i	The i-th component of σ

5. Our Secure Announcement Protocol

5.1 Proposed Model

The system is composed of four main components, namely the cloud which acts as the TP, RSUs, and vehicles ($\mathcal{V}_s$ and $\mathcal{V}_r$). To join the network, a vehicle establishes a secure channel with the cloud and receives valid credentials during the registration process to prove its authenticity. RSUs play a crucial role in transmitting information between the cloud and vehicles, and in distributing successfully validated safety messages to $\mathcal{V}_r$ in the vicinity of the reported incident. The cloud performs computations and verifies the validity of safety messages, while $\mathcal{V}_r$ uses the reliability of the received messages to authenticate secure cloud-based communication. Our protocol considers the insider threat, as insiders can attack other vehicles using their legitimate access. The threat posed by outsiders is not considered as they are less of a risk to other vehicles, and they do not possess legitimate credentials or direct network access. We assume the cloud is reliable since it cannot access a vehicle's private key. The protocol is designed to utilize the presence of cloud providers in each region, with the cloud being linked to a number of grids that divide the traffic area. A grid of a traffic area is illustrated in **Fig. 2**.

Fig. 2. Grids that represent a traffic area.

5.2 The Setup

In the setup, system parameters and credentials for the entities in the system were generated. We describe the setup of the cloud and vehicles as follow:

5.2.1 Computational Assumption and System Setup

The algorithm is based on bilinear pairing and takes input a security parameter ∄ , and outputs a public parameter $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, e)$. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be a finite cyclic group, respectively, of the same prime order, p. Assume $\mathbb{G}_1 = \langle g_1 \rangle$ and $\mathbb{G}_2 = \langle g_2 \rangle$ and $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is an efficient non-degenerate bilinear map such that $e(g_1, g_2) \neq 1$ and for all $h_1 \in \mathbb{G}_2$ and $h_2 \in \mathbb{G}_1$. Our computational assumption relies upon on Decisional Diffie-Hellman (DDH) assumption and the Diffie-Hellman Knowledge (DHK) assumption [43]. The DDH hold in $\mathbb{G}_1$ where $g, g^a, g^b, g^c \in \mathbb{G}_4$ such that $a, b, c \in \mathbb{Z}_p^*$ for any probabilistic polynomial time (PPT) adversary A, the probability decides if $c = ab$ is neglibly away from $\frac{1}{2}$. While in DHK, given $(g, g^x) \in \mathbb{G}^2$ for randomly chosen $x \in \mathbb{Z}_p^*$, it creates a Diffie-Hellman tuple (g, g^x, g^r, g^{xr}) without the knowledge of r. Then, Assume the DDH and DHK assumptions hold in $\mathbb{G}_1$ and that is computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ for instance $\phi(g_2) = g_1$. Let h_2 and U_2 be randomly chosen from $\mathbb{G}_2$ and $u, v \in \mathbb{Z}, e\left(h_{1,}^{u}\, h_2^v\right) = e(h_1, h_2)^{uv}$. The system parameters are $\mu = \langle p, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, h_1, h_2, U_1, U_v, H_1, H \rangle$.

5.2.2 Key generation and Vehicle Registration

In the following steps, a $\boldsymbol{\mathcal{V}}$ establishes communication with the cloud through a secure channel to register for a Vehicular Communication (VC) network

Step 1: $\boldsymbol{\mathcal{V}}$ self-generate a key pair $\boldsymbol{\mathcal{PK}_v}$, $\boldsymbol{\mathcal{SK}_v}$ to become a legitimate member in the network. $\boldsymbol{\mathcal{V}}$ requests validation of its self-generated public key from the cloud ($\boldsymbol{\mathcal{PK}_v}$) preserving its secret key ($\boldsymbol{\mathcal{SK}_v}$) private at time, t, where $\left(\boldsymbol{\mathcal{PK}_v} = \boldsymbol{U_1^{\mathcal{SK}_v}} \in \mathbb{Z}_{\boldsymbol{p}}^*\right)$. A vehicle generates its tracking data, $\boldsymbol{T_v} = \boldsymbol{g_2^{\mathcal{SK}_v}}$ where $\boldsymbol{g_i}$ represent random generator of $\mathbb{G}_{\boldsymbol{i}}$. Then, $\boldsymbol{\mathcal{V}}$ submit $(\boldsymbol{\mathcal{PK}_v}, \boldsymbol{\mathcal{PK}_p}, \boldsymbol{T_v},)$ to $\boldsymbol{\mathcal{TKC}}$.

Step 2: $\mathcal{TKC}$ checks for authenticity of $e(\mathcal{PK}_v, \mathcal{PK}_p, g_2) = e(U_v, U_{p,} T_v)$. Upon successful completion verification, $\mathcal{TKC}$ produces a signature on $\mathcal{PK}_v$ and forwards to $\mathcal{V}$. $\mathcal{TKC}$ then saves data of ($\mathcal{PK}_v, \mathcal{PK}_p, T_v$) via its internal system.

Step 3: The vehicle, denoted by $\mathcal{V}$, undergoes the Zero-Knowledge Proof Protocol (ZKPP) represented as $\mathcal{ZK}\{\mathcal{SK}_v | \mathcal{PK}_v = U_1^{\mathcal{SK}_v}\}$ with $\mathcal{RGC}$ in subsequent phases. The $\mathcal{RGC}$ verifies the vehicle's authenticity by examining the signature on $\mathcal{PK}_v$. $\mathcal{RGC}$ has a key pair $(\mathcal{A}, \mathcal{Z}) = (e(\mathcal{Z}, g_2), \mathcal{Z})$, which is used to validate $\mathcal{TKC}$'s signature on $\mathcal{PK}_v$. $\mathcal{RGC}$ checks the validity of ZKPP performed by $\mathcal{V}$ and runs the computation to obtain $K_1 = g_1^k$, $K_2 = Z(h_1 \mathcal{PK}_v)^{-k}$ where $k \in \mathbb{Z}_p^*$. After successful computation, $\mathcal{RGC}$ distributes $K_v = (K_{1,} K_2)$ to legitimate vehicles. The vehicle verifies the signature by checking $e(K_{2,} g_2) e(K_{1,} h_2) e(K_1^{\mathcal{SK}_v}, U_2) = A$. If the check is successful, the vehicle can use K_v as a group certificate across the network and is registered to the cloud. The vehicle can sign any safety message using its $\mathcal{SK}_v$.

5.2.3 Message Transmission

In this phase, $\mathcal{V}$ generates a message that is related to safety and sends it to nearby vehicles through RSUs. The following information provides further details on this process:

Step 4: $\mathcal{V}$ creates the message denoted as ($\mathcal{m}$) where $\mathcal{m} = (\mathcal{MB}, t_s, loc_v, GI_v, I_{RSU})$. $\mathcal{MB}$ represents for message's broadcast type, loc_v indicates for current position of the moving vehicle, while t_s stands for the signature creation time to guarantee message freshness. Let GI_v be a group identifier for the vehicle that allows one to determine the group to which the vehicle corresponds. The symbol for RSU's actual identification is I_{RSU}.

The group signature method enables a group member to sign a message on behalf of the whole group, and the signature can be verified using a specific public key group without revealing the signer's identity. The group signature comprises three main parts, which are:

1. Randomize K_v where $\mathcal{V}$ computes $\sigma_1 = K_1 g_1^s$, $\sigma_2 = K_2 (h_1 \mathcal{PK}_v)^{-s}$ for a randomly chosen $s \in \mathbb{Z}_p^*$.

2. Randomize $\mathcal{PK}_v$ where, $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$ and generate a unique identifier for the message $\sigma_4 = H_1(\mathcal{m})^{\mathcal{SK}_v}$.

3. Generate the group signature using $\mathcal{SK}_v$ in $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$ and $\sigma_4 = H_1(\mathcal{m})^{\mathcal{SK}_v}$. $\mathcal{V}$ executes executes zero knowledge proof to persuade the verifier that a particular information is true while keeping all other information secret.

To generate a group signature, $\mathcal{V}$ evaluates:

- Set up in random for $r \leftarrow \mathbb{Z}_p^*$.
- Compute $R_1 = H_1(\mathcal{m})^r$ and $R_2 = \sigma_1^r$.
- Obtain a challenge of R_1 and R_2 where $\sigma_5 = H(\mathcal{m} || \sigma_1 || \sigma_2 || \sigma_3 || \sigma_4 || R_1 || R_2)$.
- Response to the challenge with $\sigma_6 = r - \sigma_5^{\mathcal{SK}_v} \bmod p$ and output the group signature

as $\boldsymbol{\sigma} = (\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}, \ldots, \boldsymbol{\sigma_6})$ of $\boldsymbol{m}$.

$\boldsymbol{\mathcal{V}}$ broadcasts a message tuple, $\boldsymbol{\mathcal{M}} = (\boldsymbol{m}, \boldsymbol{\sigma})$, to other vehicles via RSUs. The tuple includes a message link-identifier, $\boldsymbol{\sigma_4}$, which can only be generated once by $\boldsymbol{\mathcal{V}}$ for the same message. The RSU is used to broadcast messages from $\boldsymbol{\mathcal{V}}$ to the authentication cloud and $\boldsymbol{\mathcal{ATC}}$.

Step 5: The RSU sends $\mathcal{M}$ to the $\mathcal{ATC}$ to verify the authenticity of safety messages. The RSU prohibits communications containing the same σ_4 component to prevent the repetition of messages signed by the same vehicle. Upon successful verification, the $\mathcal{ATC}$ verifies a specific number of communications related to the same incident.

5.2.4 Message validation

After receiving the message, the cloud executes the following procedures:

Step 6: To verify the message, the cloud performs the following steps:

$\mathcal{ATC}$ checks $e(\sigma_{2,}g_2)e(\sigma_{1,}h_2)e(\sigma_3, U_2) = A$ to confirm the authenticity of the group certificate. and validate $\sigma'_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4 \,||H_1(m)^{\sigma^6}{\sigma_4}^{\sigma^5}||\,{\sigma_1}^{\sigma^6}{\sigma_3}^{\sigma^5})$.

When the message's freshness is maintained, $\mathcal{ATC}$ determines that a message is trustworthy if and only if $\sigma'_5 = \sigma_5$. Furthermore, our protocol uses adaptable threshold authentication, where the authenticity of a message is determined by the $\mathcal{ATC}$ based on the number of messages it has received reporting similar events.

Step 7: $\mathcal{ATC}$ transmits the safety message, $\mathcal{M}$, to a nearby RSU upon success verification.

Step 8: The RSU disseminates the safety message $\mathcal{M}$ to nearby vehicles in the area of the reported incident.

Step 9: $\mathcal{V}$ analyzes t_s to verify the content of the safety message. The message is considered reliable if both message verification tests pass and t_s is valid. $\mathcal{V}$ selects a random s and computes $x = h(s)$, where x represents knowledge of s without revealing it, to ensure that the message is trustworthy and validated by $\mathcal{ATC}$. V then calculates the challenge $f = (s, \mathcal{PK})_{\mathcal{ATC}}$ and sends it to $\mathcal{ATC}$. Here, h is a one-way hash function and $\mathcal{PK}_{\mathcal{ATC}}$ represents the public key of $\mathcal{ATC}$. In response to the challenge, $\mathcal{ATC}$ decrypts f to obtain s', computes $x' = h(s)'$, and terminates if $x' \neq x$, indicating that $s' \neq s$. Otherwise, $\mathcal{ATC}$ sends $s = s'$ back to $\mathcal{V}$. Consequently, $\mathcal{V}$ successfully authenticates $\mathcal{ATC}$ by verifying that the received s matches the one that was agreed upon earlier.

5.2.5 Vehicle Tracking and Revocation

Step 10: If a $\mathcal{V}$ participates in malicious activity within the network, it can be traced and detected.

Step 11: The $\mathcal{TKC}$ checks the authenticity and consistency of message $\mathcal{M}$ to revoke $\mathcal{V}$ if there is any misconduct. It is noteworthy that $\mathcal{TKC}$ has access to the trapdoor's information related to $\mathcal{PK}_{\mathcal{V}}$. To identify $\mathcal{PK}_{\mathcal{V}}$associated with $\mathcal{V}$'s identity for law enforcement and revocation purposes, the $\mathcal{TC}$ searches its local database.

6. Performance Evaluation

6.1 Security Analysis

This section examines the security concerns with our presented protocol and evaluates its efficiency. We compare our scheme with those presented in [40], [46] and [47] because those schemes proposed the authenticated anonymous announcement protocol in VC. In order to implement VC, it is indispensable that the following security requirements be met:

Reliability. All the schemes satisfy the first two requirements of message integrity and reliability of user identity. Message authentication is often achieved via a secure digital signature. The validity of the message is preserved, and messages announced without modification are guaranteed. Our protocol satisfies the requirements of user authenticity and data integrity as messages are signed with legitimate credentials provided by the cloud.

In contrast, [40, 46, 47] do not satisfy the third requirement for message reliability since no technique for measuring message reliability was put forward. Additionally, because the origin of the message in [40, 46, 47] cannot be distinguished, the threshold technique cannot be adopted. Our approach ensures the required threshold authentication property by utilizing a flexible threshold technique, which enables the cloud to determine the suitable threshold based on the message's content and location. For instance, in a highly populated city with heavy traffic, the threshold can be set higher than in a rural area with lighter traffic.

Claim 1. The proposed protocol achieves the third requirement of message reliability.

Proof: The property of threshold technique is satisfied in this protocol. To resolve the requirement of threshold authentication, we give an example of how threshold authentication technique being adopted in our scheme as below:

We let $\mathcal{V}$ receive a safety-related message, $\mathcal{M} = (m, \sigma)$ via RSU, $\mathcal{V}$ then forward $\mathcal{M}$ to $\mathcal{ATC}$via RSU. When a message is received, the $\mathcal{ATC}$ verifies the legitimacy of the vehicle in the network by checking the message-link identifier, σ_4. If the vehicle has not signed the message more than once, then $\mathcal{ATC}$ verifies the message. Otherwise, $\mathcal{ATC}$ rejects the messages. Assume, the message is valid then $\mathcal{ATC}$ waits to predefined number of reports for the same events. Subsequently, $\mathcal{ATC}$ checks for duplicate signature on the same message, $\mathcal{ATC}$ would log and discard the message if found dishonest.

Next, $\mathcal{ATC}$ receives (say n) more messages (m_i, σ_i), $1 \leq i \leq n$. If these n signatures are valid and if n satisfies the threshold, $\mathcal{ATC}$ believes that the reported event is true and disseminate to the vehicles via RSU. When the threshold is not exceeded, the messages will be added to the "waiting list" and deleted at some point in time.

If the messages are not valid then the messages will be added to the "false list" and discarded at the expiration time.

Claim 2. The proposed protocol has high robustness against impersonation attack and forgery of partial signature.

Proof: In our proposed protocol, cloud performs the issuance, distribution and management of credentials to legitimate vehicles. We evaluate the robustness of our scheme against

impersonation attack for insider. In this attack, an adversary masquerade as a legitimate vehicle. An outsider is not taken into account as they pose a lower risk to other users within the network. Suppose an adversary impersonate as an honest vehicle:

I. An adversary randomly chooses an integer $\mathcal{SK}'_{\mathcal{V}}$ for a random value, $\mathcal{SK}_{\mathcal{V}} \in \mathbb{Z}_p^*$, and let $\mathcal{PK}'_{\mathcal{V}} = U_1^{\mathcal{SK}'_v}$.
II. The signing protocol for the message, m is executed.
III. A fake message $\mathcal{M}' = (m', \sigma')$ is announced.

Let adversary be $\mathcal{A}$ and challenger be $\mathcal{C}$. Assume adversary $\mathcal{A}$ is able to forge the valid signature to manipulate other entity in the network without the fear of being arrested. If $\mathcal{A}$ intends to access the network, $\mathcal{A}$ requests the system parameters μ and thus, $\mathcal{C}$ deliver μ to $\mathcal{A}$ where:

$$\mu = \langle p, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, h_1, h_2, U_1, U_v, H_1, H \rangle. \quad (1)$$

Meanwhile, $\mathcal{C}$ generate $\mathcal{RTC}$'s public key denoted as A then forward A to $\mathcal{A}$. When $\mathcal{A}$ query a group certificate and the signature of $\mathcal{PK}'_{\mathcal{V}}$ from $\mathcal{TKC}$, $\mathcal{C}$ generate the group certificate given that $\mathcal{C}$ know the valid key pair of $\mathcal{A}$, $(\mathcal{PK}'_{\mathcal{V}}, \mathcal{SK}'_{\mathcal{V}})$. In addition, $\mathcal{C}$ possess a knowledge of $\mathcal{RTC}$'s secret key, Z to satisfy $e(Z, g_2)$. $\mathcal{C}$ learn the value of Z, except the value of $\mathcal{SK}_{\mathcal{V}}$. In order to get the value of $\mathcal{SK}_{\mathcal{V}}$, $\mathcal{C}$ run a zero-knowledge proof $\mathcal{ZK}\{\mathcal{SK}_v | \mathcal{PK}_v = U_1^{\mathcal{SK}_v}\}$ with $\mathcal{A}$ by invoking $\mathcal{A}$ twice.

Assume, $\mathcal{A}$ able to impersonates legitimate vehicle's identity which has a group signature $\sigma = (\sigma_1, \ldots, \sigma_6)$. Then, the tracking data in the name of false vehicle's certificate does not hold $e(\sigma_2, g_2) = e(\sigma_1, T_v)$. The challenger $\mathcal{C}$ firstly sends $\mathcal{SK}_{\mathcal{V}}$ to the $\mathcal{TKC}$. The $\mathcal{TKC}$ randomly chooses a secret integer $T'_v \in \mathbb{Z}_p^*$, and send T'_v to $\mathcal{C}$. Then $\mathcal{C}$ computes $T'_v = g_2^{\mathcal{SK}'_v}$. If the equation $T'_v = g_2^{\mathcal{SK}'_v}$ equal to $T_v = g_2^{\mathcal{SK}_v}$ for a same period, t. Then, $\mathcal{C}$ checks the verification equation:

$$\sigma_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4||H_1(m)^{\sigma_6}\sigma_4^{\sigma_5} \; ||\sigma_1^{\sigma_6} \, \sigma_3^{\sigma_5}) \quad (2)$$

If the equation holds the signature is valid and vice versa. Then, $\mathcal{A}$ executes the signing protocol. Note that the equation implies $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_{6)}$ is a signature on message m under one-time public key $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$, $\sigma_4 = H_1(m)^{\mathcal{SK}_v}$. When $\mathcal{A}$ requests a group signature on m, it can always be detected by $\mathcal{TKC}$. Hence, $\mathcal{A}$ fails to impersonate an identity and incapable to broadcast bogus message $\mathcal{M}' = (m', \sigma')$. Therefore, our protocol is resilient to impersonation attacks.

Privacy. We discuss two aspects of privacy: anonymity and unlinkability. The necessity of privacy is met in [40, 46, 47] by using pseudonyms where it prevents the matching of the real identification from its source. Additionally, we ensure that there is no linkability between different messages that originate from the same source. This guarantees the privacy requirement is met in our protocol.

Claim 3. Our protocol achieves authenticated privacy requirement.

Proof: When the actual identity is transmitted to the network in plaintext, the adversary can

easily obtain the actual identity of a sender by intercepting the message. Let adversary be $\mathcal{B}$, assume there have two honest vehicles denoted as $\mathcal{D}_0$ and $\mathcal{D}_1$.

We assume the adversary $\mathcal{B}$ owns the legitimate key pair $(\mathcal{PK}_v, \mathcal{SK}_v)$. and obtain the system public parameter, $\mu = \langle p, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, h_1, h_2, U_1, U_v, H_1, H \rangle$. The adversary $\mathcal{B}$ randomly chooses two different messages which are indicated as m_0 and m_1 and selects the random bit $b \in \{0,1\}$. Then, $\mathcal{B}$ forward m_b and m_{1-b} to $\mathcal{D}_0$ and $\mathcal{D}_1$ respectively. Note that, b is unknown to us. The $\mathcal{D}_0$ and $\mathcal{D}_1$ generate two legitimate signatures σ_b and σ_{1-b} which are associated to the message m_0 and m_1. We forward in random order the two signatures σ_b and σ_{1-b} to $\mathcal{B}$, otherwise return invalid symbol $\perp$ to the $\mathcal{B}$.

When adversary $\mathcal{B}$ obtains the signature, $\mathcal{B}$ computes the signature and produce b' of b, $b' \in \{0,1\}$. We declare failure if $\mathcal{B}$ can guess the value of $b' = b$. However, given one valid message and two vehicles in the network, $\mathcal{B}$ can only decide the originator of the message with a probability non-negligibly greater than $\frac{1}{2}$ in polynomial time. This is comparable to the random guess of b. Hence, we prove that our scheme fulfils the authenticated privacy requirement.

Accountability. Throughout the case of traffic collisions and incidents, evidence should be collected for the verification and settlement of claims for the assessment of liability. If some entity has unlawful actions, TP can trace the true origin of that vehicle. When malicious activity is detected later, TP has evidence to revoke the presence of vehicle in the network.

Claim 4. If there are fraudulent behaviour on a certain vehicle, TP may reveal the true identity.

Proof: When a certain vehicle is behaving maliciously, then $\mathcal{TKC}$ in this scheme can identify the real identity of vehicle. Recall that, the part of the signature under a one-time public key shows that $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$ and $\sigma_4 = H_1(m)^{\mathcal{SK}_v}$ where $\mathcal{SK}_v$ is the secret key of some group member. Hence, with the tracing information $T_v = g_2^{\mathcal{SK}_v}$ the $\mathcal{TKC}$ can trace the signer by checking $e(\sigma_2, g_2) = e(\sigma_1, T_v)$. This property allows the prosecutors to locate and detect fraudulent messages that prohibit cheating vehicles. If the same signer signs the same message twice, both signatures then hold the similar element $\sigma_4 = H_1(m)^{\mathcal{SK}_v}$. Hence, the signer may be computationally related by evaluating two signatures with the same message. This gives evidence to the $\mathcal{TKC}$ to revoke the participation of the signer from the network.

We demonstrate that the security requirements in VC network are satisfied by our security analysis. **Table 2** provides an overview of our security analysis results. Our protocol effectively addresses the requirements for message reliability, privacy, and accountability. In conclusion, our scheme appears to be more effective and resilient than the protocol proposed in the [40, 46, 47].

Table 2. Security Analysis in VC

Security Requirement	**Security Component**	[40]	[46]	[47]	Our protocol
Reliability	Authenticity of sender	√	√	√	√
	Message integrity	√	√	√	√
	Message truthfulness	X	X	X	√
Privacy	Anonymous	√	√	√	√
	Unlikable	√	√	√	√

Accountability	Traceable	√	√	√	√
	Non repudiate	X	X	X	√
	Revocability	X	X	X	√

6.2 Performance Analysis

With reference to [40, 46, 47] we compare the performance efficiency of our proposed protocol in this section. We compare our protocol to other schemes based on three criteria: the size of the message and signature, computational expenses, and execution time.

Message and Signature Size. We have chosen for the National Institute of Standards and Technology (NIST) curve [45] and a 160-bit prime for p to achieve an 80-bit security level, with the $\mathbb{G}_1$ element being 160 bits long. Our message consists of a payload, a timestamp, a group ID, and the real RSU's identity. By allocating 80 byte, 1byte, 1 byte, and 1 byte, respectively, a vehicle-generated message with an 80-bit security level has a length of 211 bytes. By contrast, the message lengths in [40], [46] and [47] are 300, 280, and 350 bytes, respectively. Our method employs a group signature with a signature size of 128 bytes. Therefore, compared to [40, 46, 47] our protocol effectively achieves lower communication costs and is acceptable for VC networks. This is illustrated in **Fig. 3**.

Computational expenses. In the process of message broadcast, we analyse and assess the computational complexity associated with both signature generation and verification. To simplify the comparison, we focus on the computational costs of scalar multiplication in $\mathbb{G}_1$ and pairing evaluation. Exponentiation is considered and converted to scalar multiplication if it is used. We compare the computational costs of our proposed method with those of [40, 46, 47]. According to [2], one exponentiation in $\mathbb{G}_\mathbb{T}$ is equivalent to about four scalar multiplications in $\mathbb{G}_1$ in the standard implementation. Therefore, we convert the cost of exponentiation to scalar multiplication in **Table 3**. Furthermore, the overhead of a multi-base pairing is approximately the same as that of a single-base pairing. Now, in order to complete the performance analysis, we add the "signature check" and "verification check" operations. In this table, $e.\mathbb{G}_1$ indicates e scalar multiplications in $\mathbb{G}_1$, $\oint.P$ signifies $\oint$ operations for pairing. The process of signing in [40] involves two scalar multiplications, while the verification process requires one pairing and three scalar multiplications. In contrast, the signing process in [46] requires two pairings and five scalar multiplications, with the verification process requiring one pairing and six scalar multiplications. In [47], the signing process requires two pairings and seven scalar multiplications, with the verification process requiring two pairings and four scalar multiplications. For our proposed protocol, the signing process involves six scalar multiplications, while the verification process involves one pairing and four scalar multiplications. **Table 3** summarises these results. We note that the computational expense of our scheme is equivalent to that of the [40, 46, 47] schemes.

Execution time. To evaluate the execution time of our proposed method, we relied on the implementation results presented in previous studies [2, 45], which showed that a single multiplication in $\mathbb{G}_1$ and one pairing evaluation can be completed within 0.6 ms and 4.5 ms, respectively, to achieve an 80-bit security level. These results were obtained by running an Intel Pentium IV 3.0 GHz which has similar performance to the CVIS vehicle machine developed for future communications in VC [2]. Using this information, we calculated the computation time required for the operations listed in the computational cost column of **Table 3**. The results of our execution time calculations are presented in the computation time column of **Table 3**. Based on these results, we conclude that our proposed method has the most

efficient communication cost when compared to [40, 46, 47]. Our proposed method achieves the lowest communication cost and outperforms the other studies in terms of computing cost and time. Furthermore, our proposed method meets all necessary security requirements for the successful implementation of an announcement protocol in VC. The overall performance of our proposed method is presented in **Table 2** and **Table 3**.

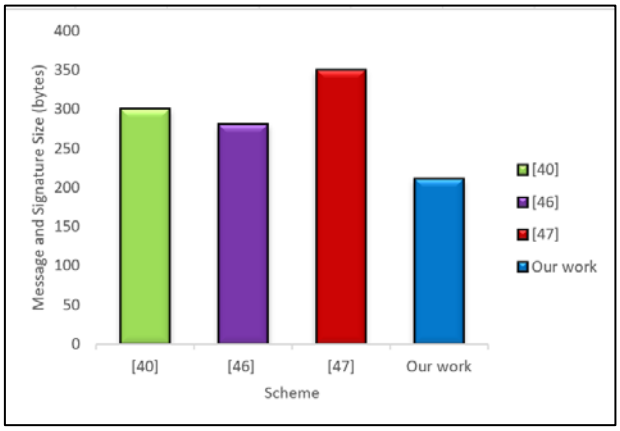

Fig. 3. The message and signature size of our protocol compared with [40, 46, 47].

Table 3. Comparison of Performance Analysis

Scheme	Message and Signature Size	Computational cost		Execution time (ms)	
		Message Signature	Message Verification	Message Signature	Message Verification
[40]	300 Bytes	$2.\mathbb{G}_1$	$1.P + 3.\mathbb{G}_1$	1.2	6.3
[46]	280 Bytes	$2.P + 5.\mathbb{G}_1$	$1.P + 6.\mathbb{G}_1$	12	8.1
[47]	350 Bytes	$2.P + 7.\mathbb{G}_1$	$2.P + 4.\mathbb{G}_1$	13.2	11.4
Our work	211 Bytes	$6.\mathbb{G}_1$	$1.P + 4.\mathbb{G}_1$	3.6	6.9

6.3 Simulation

In this section, we conducted simulations to demonstrate the feasibility of our scheme in a real-world scenario, implemented using cryptographic library MIRACL [2] and the NS-2.35 network simulator. The simulations were performed on a Linux machine running an Intel Core i5-4790 processor at a frequency of 3.6 GHz. We evaluated performance of our scheme in the context of V2V communication, using metrics such as average transmission message delay in VC (MD_{vc}) and average message loss rate in VC (ML_{vc}). We assume that the vehicular nodes were randomly distributed. To evaluate our performance metrics, we developed a formulation such a way:

$$MD_{vc} = Avg \sum_{i=1}^{N_v} Avg \left(\frac{M_{sent_i} \times T_{sign}}{M_{received_i}} \right)$$

$$ML_{vc} = Avg \sum_{i=1}^{N_v} \frac{M_{received_i} \times T_{verify}}{N_c \times N_v}$$

In this simulation, we consider the number of vehicles and cloud as N_v and N_c, respectively. Meanwhile, M_{sent} is amount of message that have been transmitted and $M_{received}$ known as amount of message that have been received. T_{sign} represents the total time taken for signature generation, while T_{verify} denotes the total time taken for signature verification. This protocol was simulated under the following design settings:

Table 4. Simulation Parameters

Parameters	**Value**
Wireless Network	IEEE 802.11a
Size of region	$2.5\ X\ 2\ .5km^2$
Execution duration	$210\ s$
The number of vehicles	10-80
Velocity of vehicles	$Min: 0\ m/s\ \ Max: 55\ m/s$
Bandwidth	6 Mbps
Messaging frequency	20 Msg/s

The simulation results are shown in **Fig. 4** and **Fig. 5** for VC communication. **Fig. 4** shows the simulation result of the correlation between the number of vehicles and the average message delay. According to **Fig. 4**, we can see that the average transmission delay rises proportionally with the growth of vehicle density. As the number of vehicles increases, the number of messages generated and broadcasted also increases, causing congestion to the network channel. As a result, this congestion leads to message transmission delay as vehicles experience interference caused by other vehicle's transmission. We can infer that our proposed protocol has an advantage over other schemes as our work yields the lowest message delay, followed by [40, 46, 47].

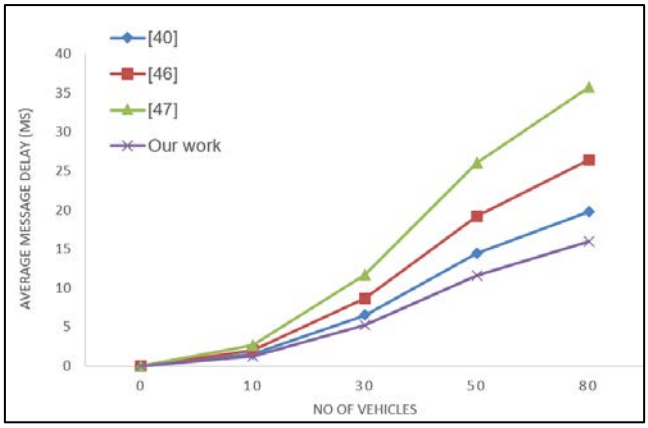

Fig. 4. The correlation between the number of vehicles and the average message delay.

The results in **Fig. 5** demonstrate that the average message loss rate increases as the number of vehicles in the network increases. This is understandable since the increase in the number of messages transmitted requires more cryptographic computations to be performed in order

to verify the messages received. These computations can lead to network congestion, resulting in messages being dropped if they are not verified before a certain time interval elapses. Our scheme is shown to have comparable or better message loss performance than the schemes proposed in [40, 46, 47].

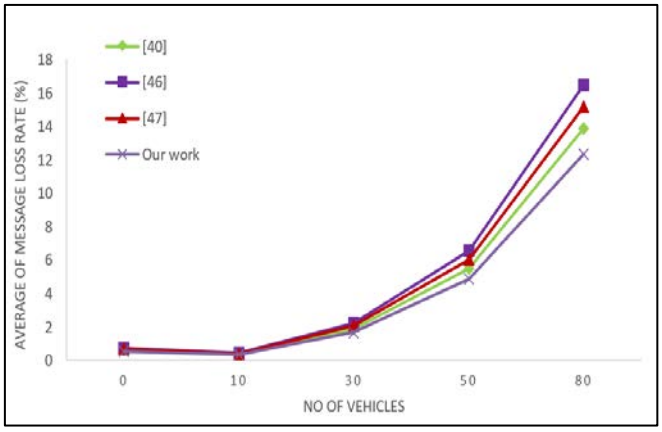

Fig. 5. The correlation between the number of vehicles and the average message loss rate.

7. Conclusion

In this study, we introduce a new protocol for privacy-preserving authentication in VC based on group signature. According to our knowledge, this is the first generic abstraction for the announcement protocol using group signatures in VC has been proposed in literature, which can serve as a guideline for designing future protocols. Our proposed protocol addresses the conflicting security requirements, providing a reliable announcement protocol while protecting user privacy against adversaries. Implementation of our protocol on NS-2.35 simulator demonstrates its practicality and suitability for real-world deployment.

Future work may aim to expand the present protocol so that more vehicles can receive a message in a larger area without compromising security. Additionally, it would be interesting to investigate the formal definitions of various security properties desired in VC and provide rigorous proofs for the security of the proposed announcement protocol in VC networks.

References

[1] WHO. Global status report on road safety, 2015. [Online]. Available: https://www.who.int/violence_injury_prevention/road_safety_status/2015/en/ (accessed on 14 January 2019).

[2] L. Chen, S. Ng, and G. Wang, "Threshold anonymous announcement in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 605-615, 2011. Article(CrossRef Link)

[3] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for vehicular ad hoc networks," *IEEE Trans. Veh. Tech.*, vol. 61, no. 9, pp. 4095-4108, 2012. Article(CrossRef Link)

[4] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Veh. Commun.*, vol. 4, pp. 30-37, 2016. Article(CrossRef Link)

[5] A. Malip, S.-L. Ng, and Q. Li, "A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks," *Sec. and Commun. Netw.*, vol. 7, no. 3, pp. 588-601, 2014. Article(CrossRef Link)

[6] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wir. Commun.*, vol. 13, no. 5, pp. 8-15, 2006. Article(CrossRef Link)
[7] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access.*, vol. 4, pp. 5356-5373, 2016. Article(CrossRef Link)
[8] Coutinho, R.W.L.; Boukerche, A. "Guidelines for the Design of Vehicular Cloud Infrastructures for Connected Autonomous Vehicles," *IEEE Wirel. Commun.*, vol. 26, pp. 6–11, 2019. Article(CrossRef Link)
[9] C. R. Storck and F. de L. P. Duarte-Figueiredo, "A 5G V2X ecosystem providing internet of vehicles," *Sensors*, vol. 19, no. 3, p. 550, 2019. Article(CrossRef Link)
[10] A. A. Ahmad, B. Colin, and G. N. J. M, "Geoproof: Proofs of geographic location for cloud computing environment," in *Proc. of the 32nd Inter. Conf. on Dist. Comp. Syst. Work.*, pp. 506 - 514, 2012. Article(CrossRef Link)
[11] M. A. Alzain, B. Soh, and E. Pardede, "A survey on data security issues in cloud computing: From single to multi-clouds," *J. of Soft.*, vol. 8, no. 5, pp.1068-1078, 2013. Article(CrossRef Link)
[12] Y. Argawal, K. Jain, and O. Karabasoglu, "Smart vehicle monitoring and assistance using cloud computing in vehicular ad hoc networks," *Inter. J. of Trans. Sci. and Tech.*, vol. 7, pp.60-73, 2018. Article(CrossRef Link)
[13] I. T. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Proc. of 2008 Grid Computing Environments Workshop*, pp. 1-10, 2008. Article(CrossRef Link)
[14] K. Z. Ghafoor, K. A. Bakar, M. A. Mohammed, and J. Lloret, "Vehicular cloud computing: Trends and challenges," in *Mob. Netw. and C.Comp. Conv. for Prog. Ser. and App.*, 2013, pp. 262-274. Article(CrossRef Link)
[15] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - the business perspective," *Dec. Supp. Sys.*, vol. 51, no. 1, pp. 176-189, 2011. Article (CrossRef Link)
[16] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Par. Distr. Sys.*, vol. 25, no. 2, pp. 384-394, 2014. Article (CrossRef Link)
[17] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Fut. Gen. Comp. Sys.*, vol. 28, no. 3, pp. 583-592, 2012. Article (CrossRef Link)
[18] R. Hussain, F. Abbas, J. Son, and H. Oh, "Tiaas: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks," in *Proc. of 13th IEEE/ACM Inter. Symp. on Clus., C., and Grid Comp.*, pp.178-179, May 13-16, 2013. Article (CrossRef Link)
[19] R. Hussain and H. Oh, "Cooperation-aware vanet clouds: Providing secure cloud services to vehicular ad hoc networks," *J.of Info. Pro. Syst.*, vol. 10, no. 1, pp. 103-118, 2014. Article (CrossRef Link)
[20] R. Hussain, Z. Rezaeifar, and H. Oh, "A paradigm shift from vehicular ad hoc networks to vehicular ad hoc networks based clouds," *Wire. Pers. Comm.*, vol. 83, no. 2, pp. 1131-1158, 2015. Article (CrossRef Link)
[21] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging vehicular ad hoc networks with cloud computing," in *Proc. of 4th IEEE Inter. Conf. on C. Comp. Tech. and Sci. Proc.*, pp. 606-609, December 3-6, 2012. Article (CrossRef Link)
[22] S. Olariu, I. Khalil, and M. Abuelela, "Taking vehicular ad hoc networks to the clouds," *Inter. J. of Perv. Comp. and Comm.*, vol. 7, no. 1, pp. 7-21, 2011.
[23] L. Scott and D. E. Denning, "A location based encryption technique and some of its applications," *Inst.of Navi. Nat. Tech. Meet.*, pp. 734-740, 2003. Article (CrossRef Link)
[24] G. Yan, S. Olariu, and M. C. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wir.Comm.*, vol. 16, no. 6, pp. 48-55, 2009. Article (CrossRef Link)
[25] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans.Intell.Transp. Syst.*, vol. 14, no. 1, pp. 284-294, 2013. Article (CrossRef Link)
[26] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wir.Comm.*, vol. 13, no. 5, pp. 8-15, 2006. Article (CrossRef Link)

[27] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez´-Nicolas, "Balanced trustworthiness, safety and privacy in in vehicle to vehicle communications," *IEEE Trans. Veh. Tech.*, vol. 59, no. 2, pp. 559-573, 2010. Article(CrossRef Link)
[28] A. Boukerche and R. E. D. Grande, "Vehicular cloud computing: Architectures, applications, and mobility," *Comp. Netw.*, vol. 135, pp.171-189, 2018. Article (CrossRef Link)
[29] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356-5373, 2016. Article (CrossRef Link)
[30] E. Lee, E. Lee, M. Gerla, and S. Oh, "Vehicular cloud networking: Architecture and design principles," *IEEE Comm. Mag.*, vol. 52, no. 2, pp. 148-155, 2014. Article (CrossRef Link)
[31] C. Spelta, V. Manzoni, A. Corti, A. Goggi, and S. M. Savaresi, "Smartphone based vehicle to driver or environment interaction system for motorcycles," *Embed. Syst. Let.*, vol. 2, no. 2, pp. 39-42, 2010. Article (CrossRef Link)
[32] B. Ahmed, A. W. Malik, T. Hafeez, and N. Ahmed, "Services and simulation frameworks for vehicular cloud computing: A contemporary survey," *EURASIP J. Wir. Comm. and Netw.*, vol. 2019, p. 4, 2019. Article (CrossRef Link)
[33] W. He, G. Yan, and L. D. Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Trans. Indu. Infor.*, vol. 10, no. 2, pp. 1587-1595, 2014. Article (CrossRef Link)
[34] N. Kumar, S. Misra, and M. S. Obaidat, "Collaborative learning automata based routing for rescue operations in dense urban regions using vehicular sensor networks," *IEEE Syst. J.*, vol. 9, no. 3, pp. 1081-1090, 2015. Article (CrossRef Link)
[35] H. Hartenstein and K. P. Laberteaux, "VANET: vehicular applications and inter networking technologies," in *Intel. Transp. Sys.*, 2010. Article (CrossRef Link)
[36] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 834-864, 2019. Article (CrossRef Link)
[37] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," in *Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments - 15th International Conference, HCI International 2013*, Proceedings, Part II, 2013, pp. 173–180.
[38] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Tran. Intel. Trans. Syst.*, vol. 14, no. 1, pp. 284-294, 2013. Article (CrossRef Link)
[39] *C. Song*, X. Gu, L. Wang, Z. Liu and Y. Ping, "Research on Identity-based Batch Anonymous Authentication Scheme for VANET," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 12, pp. 6175-6189, 2019. Article(CrossRef Link)
[40] H. Al-Balasmesh, M. Singh, and R. Singh, "Framework of data privacy preservation and location obfuscation in vehicular cloud networks," *Concu. and Comp.: Pract. and Exper.*, vol. 34, no 5, 2022. Article (CrossRef Link)
[41] M. Raya, A. Aziz, and J. Hubaux, "Efficient secure aggregation in vehicular ad hoc networks," in *Proc. of the Third Int. Work. on Veh. Ad Hoc Net., VANET 2006*, pp. 67-75, Sept 29, 2007.
[42] L. Scott and D. E. Denning, "A location-based encryption technique and some of its applications," *Inst.of Navi. Nat. Tech. Meet.*, pp. 734-740, 2003. Article (CrossRef Link)
[43] L. Nkenyereye and K. H. Rhee, "Secure traffic data transmission protocol for vehicular cloud," *Adv. in Comp. Sci. and Ubi. Comp.*, pp. 497–503, 2015. Article (CrossRef Link)
[44] N. A. S Amir, A Malip, W. A. M Othman, "Securing Anonymous Authenticated Announcement Protocol for Group Signature in Internet of Vehicle," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, no 11, pp. 4573-4594, 2020. Article (CrossRef Link)
[45] P. Mell and T. Grance, "The NIST definition of cloud computing," *Special Publication*, vol. 800, p. 145, 2011.
[46] L. Zhang, X. Meng, K. K. R. Choo, Y. Zhang, & F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Trans. on Depend. and Sec. Comp.*, vol. 17, no 3, pp. 634-647, 2020. Article (CrossRef Link)

[47] X. Li, X. Yin, & J. Ning, "Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud," *IEEE Tran. Intel. Trans. Syst.*, vol. 24, no 2, pp. 1786-1800, 2023. Article (CrossRef Link)

Nur Afiqah Suzelan Amir received the B.Sc. (first class) degree from the University of Technology Mara, Malaysia and the M.Sc. degree in Mathematics from the University of Malaya, Malaysia. She is currently pursuing her Ph.D under the supervision of Prof Dr. Wan Ainun Mior Othman and Prof Dr. Wong Kok Bin in the University of Malaya, Malaysia. Her current research interests are cryptographic protocols and network security.

Wan Ainun Mior Othman received the M.Sc. degree in Applied Mathematics from North Carolina State University and a Ph.D. degree in Mathematics from the Universiti Sains Malaysia. She is currently an Associate Professor with the Institute of Mathematical Sciences in University of Malaya, Malaysia. Her research interests include cryptography, cryptographic applications and computational mathematics.

Kok Bin Wong received the M.Sc. degree in Mathematics from the University of Malaya, Malaysia and a Ph.D. degree in Mathematics from the the University of Malaya, Malaysia. He is currently a Professor with the Institute of Mathematical Sciences in University of Malaya, Malaysia. His research interests include applications of decision problems to cryptography, decision problems in combinatorial group theory, combinatorics.