Securing Anonymous Authenticated Announcement Protocol for Group Signature in Internet of Vehicles

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

Received July 8, 2020;accepted November 5, 2020;
published November 30, 2020

Abstract

Announcement protocol in Internet of Vehicles (IoV) is an intelligent application to enhance public safety, alleviate traffic jams and improve transportation quality. It requires communication between vehicles, roadside units and pedestrian to disseminate safety-related messages. However, as vehicles connected to internet, it makes them accessible globally to a potential adversary. Safety-related application requires a message to be reliable, however it may intrude the privacy of a vehicle. Contrarily, if some misbehaviour emerges, the malicious vehicles must be able to traceable and revoke from the network. This is a contradiction between privacy and accountability since the privacy of a user should be preserved. For a secure communication among intelligent entities, we propose a novel announcement protocol in IoV using group signature. To the best of our knowledge, our work is the first comprehensive construction of an announcement protocol in IoV that deploys group signature. We show that our protocol efficiently solves these conflicting security requirements of message reliability, privacy and accountability using 5G communication channel. The performance analysis and simulation results signify our work achieves performance efficiency in IoV communication.

***Keywords*:** Announcement, accountability, group signature, internet of vehicles, privacy, reliability.

This work was supported by the Ministry of Education Malaysia under research grant FP040-2019A.

http://doi.org/10.3837/tiis.2020.11.018 **ISSN : 1976-7277**

1. Introduction

Road traffic fatalities is one of the leading causes of injury deaths and the tenth leading cause of all deaths worldwide [1]. The growing concern in road safety and traffic efficiency has drawn a significant interest towards the development of secure vehicular communications. This drives the evolution of transportation technology known as vehicular ad hoc network (VANET). VANET guarantees a secure and efficient driving environment by enabling vehicles to communicate with each other (V2V) and infrastructure (V2I) to enhance driving safety and traffic efficiency [2-6]. However, VANET has lower capacity in terms of processing and computation for the future high-end vehicle technologies [7]. Therefore, a new paradigm shift from conventional VANET to Internet of Vehicles (IoV) was envisioned. Consider the following scenario:

"Suppose an upcoming vehicle is passing a parked vehicle in basement car park area. A pedestrian who is fully blocked by the parked vehicle intends to cross. However, neither the upcoming vehicle nor the pedestrian has an obstructed view due to the occluded parked vehicle. The parked vehicle also affects the sensors installed in the upcoming vehicle where there exists a restriction of their direct line of sight to the pedestrian. Hence, that would be a potentially dangerous situation for both upcoming vehicle and pedestrian". This instance of a scenario, gives rise to IoV (**Fig. 1**). IoV permits V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interconnectivity, thereby creating an intelligent network for each entities to communicate with each other [8-9]. With IoV paradigm, vehicles are equipped with an established internet protocol (IP) communication and data interaction standards (such as IEEE 802.11p WAVE standard, and cellular technology, e.g. 4G or 5G). Such network integration supports safety applications in particular intelligent traffic management, intelligent dynamic information service, and intelligent vehicle control [10].

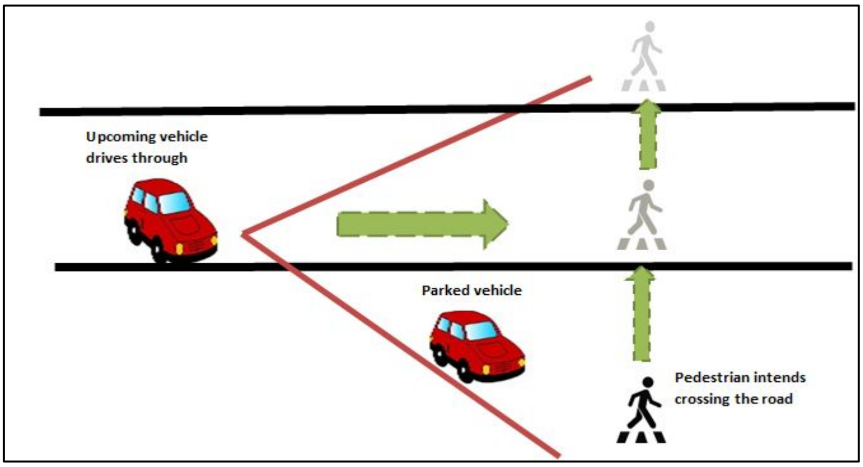

Fig. 1. A scenario in IoV

Announcement protocols in IoV permit vehicles to broadcast and inform neighbouring vehicles and pedestrians regarding safety-related announcements such as traffic delays, injuries, potholes and hazardous roadways. This enables vehicles and pedestrians to anticipate the traffic situations ahead and take actions accordingly. In order to fully utilize IoV, the transmission of safety messages must reflect the actual situations while preserving the privacy of vehicles. However, verification of message reliability may allow irresponsible parties to track vehicles or pedestrians for profiling. Profiling is the activity of collecting confidential information that may lead to the true identity of the sending vehicle. On the other hand, in a situation where a misbehaved vehicle acts maliciously, there must be a mechanism to allow the TP to trace and identify the vehicle's identification for law enforcement purposes. Furthermore, the misbehaved vehicle could not repudiate of sending the message. The presence of adversaries in the network is a common assumption in vehicular communications [2,5-6,11-12]. There are two categories of adversaries: external and internal. External adversary is a malicious entity that is not equipped with credentials to participate in the network. Meanwhile, an internal adversary is a legitimate malicious participant who possesses valid credentials issued by the TP in the network.

Security and privacy issues have attracted wide attention in IoV [12-16]. As vehicles connected to the internet, it makes them vulnerable to an adversary or malicious parties. An adversary may cause harmful effects that could potentially threaten the life of other users in the network. For instance, they may install malicious input onto vehicles and downloading infected files that may affect the whole network relatively quick [17]. If a network intrusion occurs in IoV, vehicles may be under the control of an adversary. Scalability, interoperability, reliability, efficiency, availability, and security can be challenging to achieve in IoV environment due to its globally internet connectivity.

There are a number of protocols in the literature that discusses on the matter of message reliability, privacy and accountability in IoV network [13,15-16,21-25]. A safety message is considered **reliable** if:

- Messages announced by legitimate vehicles using valid credentials provided by a trusted party (TP) in the network.
- The integrity of the message is preserved.
- The reliability of a message is measured [3, 5].

There are two aspects of **privacy**, which are anonymity and unlinkability. Anonymity indicates a sender's identity is hidden to others within the network [19]. Unlinkability implies that the activities cannot be linked to its source where an entity could not determine whether two messages originate from the same vehicle or not. In order to make the network resilient to vulnerable attacks, it must fulfil the **accountability** requirement. If any dispute arise, the misbehaved vehicle is traceable by the TP and the said vehicle could not deny having sent the message. If proven misbehaved, it will be revoked from further participation in the network [20].

Digital signature technique is commonly used to solve the first two requirements of message reliability [13,15-16,21-25]. To achieve the last requirement, the threshold method [2,18,26-28] and reputation system [3,33] are among the common techniques adopted in announcement protocols for vehicular communication. Reputation system is based on an evaluation of parameterized feedback messages represented by a numerical score. A message is considered reliable if the vehicle that generates the message has sufficient high reputation and vice versa. We focused on threshold method where an announced message is considered to be reliable if a number of different legitimate transmitters of a certain threshold reported the same event within a time interval. However, the threshold method requires distinguishability of message origin where a verifier could verify whether the same signer produces two distinct signatures on that same message and that the message can be linked. This contradicts with privacy. Hence, this presents a challenging security concern in which message reliability checks may reveal the real identity of the sender. Thus, protecting vehicle's privacy is indispensable in IoV network.

Accountability is desirable when conflict arises. However, it contradicts the privacy requirement where it allows the TP to trace and revoke a malicious vehicle by opening the signature [2,18]. Non-repudiation can be satisfied if the originator of the message disavows to send a signed message using an anonymous credential that belonged solely to the vehicle [19]. One of the common ways to revoke misbehaved vehicles is by updating and distributing certificate revocation lists (CRLs) across the network [2,5].

In this paper, we design a secure and efficient announcement protocol where our work is a modification and extension of MLGS scheme [18]. To the best of our knowledge, our work is the first comprehensive construction of an announcement protocol using group signature that resolves the conflicting security requirements of message reliability, privacy and accountability in IoV. Our contribution are as follows:

- We construct a generic abstraction of an announcement protocol for group signature. This generic abstraction aims to provide a basis for future construction of announcement protocol using group signature in IoV. As far as we are aware of, this is the first construction of such abstraction proposed in the literature for IoV.
- We design the first comprehensive construction of an announcement protocol in IoV using group signature that possesses the attractive properties of message reliability, privacy and accountability simultaneously. The main merit of group signatures based technique is that vehicles only need to store a key pair, thus it overcomes the limitation of pre-storing a large number of anonymous certificates.
- We provide an analysis that shows our protocol achieves efficient security level, system robustness and performance efficiency. We then run our protocol on a network simulator NS-2.35. This simulation demonstrates the practicality of our work in real world implementation.

The rest of the paper is structured as follows. Section II outlines related work associated schemes that present security and privacy issues in IoV. In Section III, the system and network model are presented. Section IV provides a brief review of MLGS scheme which we adopt and extend in our work. The proposed protocol is detailed in Section V. The performance and simulation of our protocol are evaluated in Section VI followed by a conclusion and future work in Section VII.

2. Related Work

Security threats and privacy issues are vital in IoV. A number of literature discussing on the security of IoV have been presented in [13,15-16,21-25]. A secure mechanism based on symmetric key cryptography to protect data privacy for big data collection in a large scale of IoV was proposed in [23]. In this scheme, each vehicle initiates a mutual authentication process with the TP and The RSU who has the HMAC encryption key is responsible to verify the authenticity of the message by computing a matching HMAC. Hence, the first two requirements of message reliability are achieved. However, it does not achieve distinguishability of message origin. This implies threshold receives a unique shared symmetric key during the registration phase. Using the symmetric key, the vehicle generates a symmetric hash message authentication code (HMAC) to sign safety messages. method cannot be incorporated in this scheme. A pair of symmetric keys to is required be created during the authentication phase before a message is broadcasted, which may result in message delay, thus increasing message drop. Furthermore, this scheme does not mention any privacy and accountability technique in its construction.

Sahbi et al. [16] presented an announcement scheme for IoV using public key cryptography. A TP generates a pair of public and private key together with its certificates during the initialization phase. The RSU is involved in message broadcast phase by assigning a pair of keys to a vehicle that enters its communication range. The vehicle then uses the pair of keys to communicate with each other in its domain. This scheme fulfils the property of message authentication. However, the third requirement of message reliability is not met where the origin of message is indistinguishable. A threshold mechanism cannot be applied in this scheme. Matter of privacy and accountability were also not discussed in [16], which may render the scheme inefficient.

In [15], an anonymous authentication protocol based on certificateless short signature scheme (CLSS) was proposed. The protocol consists of two different roles of authorities which are the transportation control centre (TCC), and the trace back authority (TBA). A vehicle signs a message using a legitimate credential issued by the TCC, therefore satisfying the requirement of message authentication. The RSU acts as a regional management. The same public and private key pairs are distributed to RSUs in the same wireless area. When a vehicle enters a new area, RSUs will issue the public key. In terms of privacy, anonymity is achieved using pseudonyms that does not contain information associated to sender. A message is signed using a one-time pseudonym, thus satisfies the unlinkability requirement. In cases where a vehicle misbehaved, the TCC forwards the revocation lists and informs TBA to identify the real identity of misbehaved vehicle. However, the origin of a message is indistinguishable. Therefore, threshold mechanism cannot be adopted and thus, message reliability is not achieved in [15].

Cui et al. [13] proposed a privacy preserving authentication using double pseudonym for IoV. This scheme adopted batch authentication to evaluate message reliability. Each vehicle generates its own pairwise public and secret key together with the corresponding certificates preloaded by TP. Signing a message using valid credentials from TP satisfy the first two requirements of message reliability. It achieves anonymity by using pseudonym. Message is linkable for a short time, where vehicles change and update pseudonym regularly. However, vehicles need to regenerate its private key whenever it wants to sign a message. This require periodic credential verification from TP, thus render [13] to be impractical. Moreover, the drawback of batch authentication is that message origin cannot be distinguished. Therefore, threshold method cannot be used to evaluate message reliability.

Liu et al. [24] designed a privacy-preserving dual authentication and key agreement (PPDAS) scheme for a secure V2V communications in IoV. An ID based authentication was presented where the TP is assumed fully trusted. Message signed using valid credentials from TP assures message authentication. Node reputation evaluation is adopted to measure the trustworthiness of the safety message where vehicle scores each other according to the reliability of message announced. The RSU is needed to generate and issue a session key to protect the privacy of the vehicle. However, this signifies computation reliance on the infrastructure. The requirement of privacy is satisfied by the use of pseudonym that is updated dynamically according to the degree of privacy required by a vehicle. Nevertheless, as this scheme assumes TP is fully trusted, the requirement of non-repudiation is not satisfied since the secret key is not exclusively belong to the signer.

In [25], Harsha et al. proposed an announcement authentication scheme for IoV based on identity based cryptography. A tamper proof device (TPD) generates pseudo-identities for each vehicle, which is used to generate a signature on a message. This satisfies the property of message authentication. Threshold adaptive authentication cannot be adopted as the origin of the message cannot be distinguished. Anonymity and unlinkability are achieved using different pseudonyms to sign messages. However, identity-based suffers key escrow problem where the TP has to be completely trusted as it is also in possession of the vehicle's private keys.

A different variation of identity based security scheme in IoV was proposed by Argawal et al. [21]. The vehicle then uses the anonymous credentials to sign a safety message. This scheme fulfils the requirement of message authentication. However, it could not distinguish whether the same vehicle signed two messages or not. This indicates threshold mechanism cannot be used. For privacy, the short term anonymous credentials are replenished whenever it enters a new RSU domain. Each vehicle generates a new secret key to sign each message. The message is then forwarded to a TP via a RSU. Thus, the properties of anonymity and unlinkability are satisfied. A TP is required to compute a private key that corresponds to a particular public key. The matching public key allows the TP to retrieve the real identity of a vehicle in case of misbehaviours. Nonetheless, this scheme requires frequent communication with TP to authenticate the credential, in which the TP might not be continuously available.

Chen et al. [13] proposed an improved authentication protocol for IoV based on identity based authentication. Each vehicle receives a smart card associated to its real identity from a TP during registration. The smart card is used as vehicle's credential to sign safety messages in IoV. Signing a message using valid credentials from a TP satisfies message authentication. A TP creates and maintains a database for every vehicle registered into the network and retrieve the real identity of a vehicle in case of misbehaviours. In terms of privacy, anonymity is achieved using smart card that undisclosed to the recipient. Messages sign using the same smart card can be connected over its relatively short life. Nevertheless, it could not differentiate whether or not two messages were signed by the same vehicle. Hence, threshold method could not be implemented throughout this scheme.

The schemes discussed in [13,15-16,21-25] does not provide a promising solution for secure authentication in IoV. The sender's legitimacy and data integrity is assured in all the IoV schemes proposed. However, the evaluation of message trustworthiness cannot be provided in [13,15-16,21-23,25]. Matter of privacy is addressed in all the IoV schemes presented except in [16]. Although misbehaved vehicle is traceable in the network, there is no explicit revocation technique discussed in [13,15-16,21-25]. Furthermore, all schemes provide non-repudiation except in [24-25]. In view of the shortcoming of the existing schemes, we propose a novel announcement protocol in IoV environment using group signature that solves the contradictory requirements of message reliability, privacy and accountability that exist in previous scheme. Finally, a comparative analysis and simulation are conducted to compare our protocol to existing schemes, and the result prove that our protocol achieves better performance efficiency in IoV communication.

3. System and Network Model

3.1 Entities

The network model consists of a cloud, roadside units (RSUs), vehicle which composed of sending vehicle (V_s) and receiving vehicle (V_r), and pedestrian (P). We introduce the role of each entity as follows:

1) **Cloud**. We rely on a cloud network that plays the role of a trusted party (TP). One of the cloud's roles is managing vehicle's admission into the system and revoking dishonest vehicles. It is accountable for the issuance and management of credentials. The identity of

a misbehaved vehicle will only be revealed by a cloud when a vehicle is found to be malicious. The cloud also computes and verifies the reliability of safety messages. This may reduce the computational burden on V_r as we utilize the functionality of the cloud.

2) **Roadside Unit (RSU).** The RSU is a physical infrastructure located along the roadsides and highways. A gradual deployment of RSUs is assumed. RSUs are expected to be densely distributed in urban areas due to the density of population in relative. Vehicles may communicate to RSUs through short range communication. The infrastructure acts as a gateway and relays the information between the cloud and vehicles. It is worth noting that our protocol does not require a confidential communication channel between the RSU and the vehicle. All RSUs are authenticated and verified by the cloud upon their participation in the network.

3) **Vehicle**. Vehicles in IoV network consist of sending vehicle (V_s) to generate and forward the safety-related messages in the network and receiving vehicle (V_r) that utilize and act accordingly upon receiving the safety messages. We assume that each vehicle in the network is equipped with a computing device called an onboard unit (OBU). An OBU has a wireless communication capability that consists of Event Data Recorder (EDR), which records received messages. The TPD is embedded as part of OBU that implements cryptographic tools and ensures authenticated access control.

4) **Pedestrian**. A pedestrian's average walking speed is 1.4 m/s (5 km/h). Pedestrians have devices such as smartphones, tablets and personal digital assistant (PDA) in IoV. Current smartphones are equipped with various sensors, which include accelerometer, GPS, and communication technologies, such as cellular (LTE or 3G), Bluetooth and Wi-Fi. Smartphones have limited computation, storage and processing capability. All the computation process are performed by the cloud.

3.1.1 Communication Channel

A fifth generation (5G) wireless technology is adopted to support V2V, V2R and V2P communications in IoV. 5G is designed to achieve high data-rates (up to 20 Gbps) and provides a latency of 1 ms for real-time applications [29]. The coverage of 5G is up to 30 km for vehicles and pedestrians to communicate.

3.2 Network Model

We formulate a generic abstraction for an announcement protocol using group signature. To the best of our knowledge, this is the first generic announcement protocol for IoV. The abstraction as depicted in **Fig. 2** consists of the following steps:

Registration Phase

Step 1: To participate in the network, V_s and P send request to acquire credential from the cloud.

Step 2: To certify V_s and P legitimacy in the network, cloud generates, issues and stores credentials in its database.

Step 3: Upon success verification, cloud returns credential to V_s and P.

Broadcast Phase

Step 4: V_s generates and relays safety message associated to the event to the cloud via RSU.

Step 5: RSU performs as a gateway between cloud and V_s where it forwards the safety message to the cloud for verification.

Verification Phase

Step 6: Cloud evaluates the reliability of the message.

Step 7: Upon success verification, cloud forwards the safety message to a nearby RSU where the reported event occurred.

Step 8: RSU broadcast the verified safety message to V_r and P in the vicinity of the event reported.

Step 9: V_r and P validate the message and utilize the safety message.

Revocation Phase

Step 10: If V_r and P experienced any misconduct from its encounter with V_s, they have the option to lodge a report to the cloud via the RSU.

Step 11: Upon receiving reports, the cloud identifies the source and integrity of the report by V_r before making a decision whether or not to revoke V_s from the network.

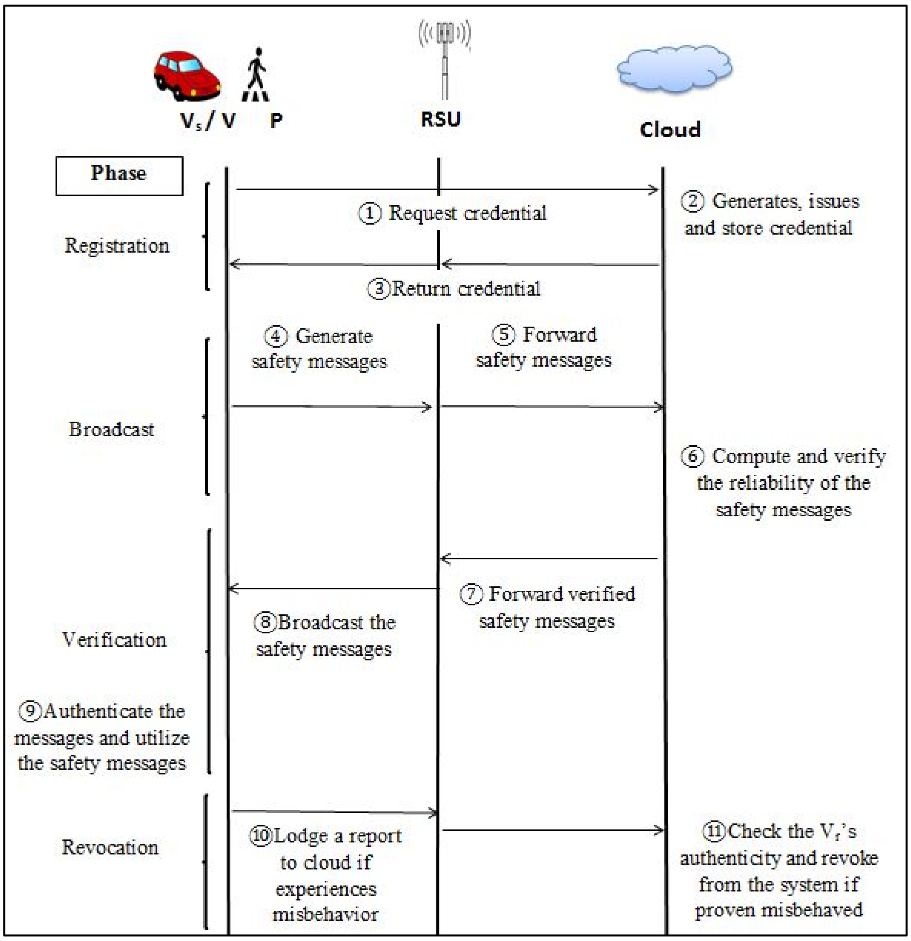
Vs / V
P
RSU
Cloud
Phase
Registration
① Request credential
② Generates, issues and store credential
③Return credential
④ Generate safety messages
⑤ Forward safety messages
Broadcast
⑥ Compute and verify the reliability of the safety messages
⑦ Forward verified safety messages
⑧Broadcast the safety messages
Verification
⑨Authenticate the messages and utilize the safety messages
Revocation
⑩Lodge a report to cloud if experiences misbehavior
⑪Check the Vr's authenticity and revoke from the system if proven misbehaved

Fig. 2. Generic Abstraction

4. The MLGS Construction

We present an overview of the MLGS scheme. Wu et al. [18] proposed a message linkable group signature (MLGS) for anonymous authentication which relies on bilinear-pairing groups and anonymous threshold authentication. This resilience approach can thwart Sybil attack as the real identity of a sender is revealed if a vehicle signs a message more than once.

In this scheme, multi-TPs were presented which are, vehicle manufacturers ($\mathcal{VM}$), a group registration manager ($\mathcal{RM}$), and a tracing manager ($\mathcal{TM}$). To participate in the network, $\mathcal{VM}$ and a vehicle signs a contract to determine that the vehicle is registered. The vehicle is then able to register to $\mathcal{RM}$ as a legitimate group member. Vehicle self-generated public key, $Y = U_1^y$ for a random value $y \in \mathbb{Z}_p^*$, where y is the vehicle's secret key. The tracing information, $T = g_2^y$ will be sent to $\mathcal{TM}$ during registration for traceability. Upon success registration in the network, $\mathcal{RM}$ issues a signature on the vehicle's public key. The signature will be used by the vehicle as a group certificate to broadcast the safety message. **Table 1** shows the lists of some notations used in our protocol which was adopted from MLGS scheme [18]. For ease of comparison, we use the same notation as [18].

Table 1. Table of Symbol and Notation

Notation	Description
$\mathcal{TC}$	Tracing cloud
$\mathcal{RC}$	Registration cloud
$\mathcal{AC}$	Authentication cloud
$\mathcal{V}$	Vehicle
$\mathcal{P}$	Pedestrian
$\mathbb{G}_i (i = 1,2,3)$	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
$\mathcal{PK}_p$, $\mathcal{SK}_p$	$\mathcal{P}$'s key pair
MT	Message type
GID_v	Group ID of the vehicle
ID_{RSU}	Real identity of RSU
$K_v = (K_1, K_2)$	The group certificate of vehicle
K_p	The group certificate of pedestrian
$T_v = g_2^{\mathcal{SK}_v}$	The tracing information of vehicle
$T_p = g_3^{\mathcal{SK}_p}$	The tracing information of pedestrian
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 Proposed Protocol

5.1 System Architecture

The system consists of four parties, which are the cloud, roadside units, vehicles and pedestrian. A vehicle communicates with the cloud via a confidential channel to enrol into the network. During the registration process, cloud certifies the legitimacy of each vehicle and RSU by secure distribution of valid credentials in the network. The involvement of RSU is needed to relay information and perform as a gateway between the cloud and a vehicle. Cloud performs the computation process and verifies the reliability of the safety messages. The RSU disseminate the successful verified messages to $\mathcal{V}_r$ and pedestrian in the proximity of event reported. A $\mathcal{V}_r$ and a pedestrian then utilize the reliability of messages received and verify that the message is reliable from cloud.

We consider the presence of internal adversaries in our protocol. An internal adversary may manipulate their legitimacy to conduct attacks on other vehicles. External adversary is not being considered as they pose less harm to other vehicles since they do not possess valid credentials or direct access to participate into the network. We assume the cloud is semi-trusted as they have no access to a vehicle's and pedestrian's secret key.

We consider smartphone as the most widely accepted choice of a pedestrian's device. This is due to their versatility and ubiquitous features it possesses. Smartphone has limited resources in terms of computation power and storage. As the cloud has extensive computing resources that can be allocated on demand, it performs the computation process and verifies the reliability of the safety messages. A typical safety message contains message type, location and direction of the respective vehicle or pedestrian. This safety information can be utilized by the pedestrian to be aware of the situation ahead of them and as a result, may reduce the number of road casualties. Vehicles may transmit 5 safety messages per second (i.e., at fixed 5 Hz frequency). To estimate storage requirement, consider smartphone capability of one month with 10 safety messages updates per minute. A total of 30.24.60.10 = 432,000 one-time certificates will be required. Hence, we can conclude each smartphone approximately requires 432 KB of storage to run up this safety application. This is reasonable storage for modern smartphone with current technology [30].

5.1.1 Computational Assumptions and System Setup

Our protocol setup algorithm is based on bilinear pairing and takes input a security parameter $\nexists$, and outputs a public parameter $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, g_3, e)$. 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 $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ 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 scheme is based on Decisional Diffie-Hellman (DDH) assumption and the Diffie-Hellman Knowledge (DHK) assumption [31]. 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 decide 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.

We assume the DDH and DHK assumptions hold in $\mathbb{G}_1$. We assume 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 $\mu = \langle p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, g_3, e, h_1, h_2, h_{3,} U_1, U_v, U_{p,} H_1, H \rangle$.

5.2 Vehicle and Pedestrian Registration

To register to a IoV network, a vehicle communicates with the cloud via a confidential medium in the subsequent steps:

Step 1: To participate in the network, $\mathcal{V}$ self-generate a key pair $\mathcal{PK}_{\mathrm{v}}$, $\mathcal{SK}_{\mathrm{v}}$. $\mathcal{V}$ sends request to the cloud to certify its self-generated public key ($\mathcal{PK}_{\mathrm{v}}$) while keeping its private key ($\mathcal{SK}_{\mathrm{v}}$) private at time t, where $\left(\mathcal{PK}_{\mathrm{v}} = \mathrm{U}_{\mathrm{v}}^{\mathcal{SK}_{\mathrm{v}}} \in \mathbb{Z}_{\mathrm{p}}^{*}\right)$. For pedestrian registration, $\mathcal{P}$ self-generate a key pair $\mathcal{PK}_{\mathrm{p}}$, $\mathcal{SK}_{\mathrm{p}}$ where $\left(\mathrm{P}\mathcal{K}_{\mathrm{p}} = \mathrm{U}_{\mathrm{p}}^{\mathcal{SK}_{\mathrm{p}}} \in \mathbb{Z}_{\mathrm{p}}^{*}\right)$ and forwards the request to cloud to certify its self-generated public key ($\mathcal{PK}_{\mathrm{p}}$) while keeping its secret key ($\mathcal{SK}_{\mathrm{p}}$) confidential. A vehicle computes its tracing information $\mathrm{T}_{\mathrm{v}} = \mathrm{g}_2^{\mathcal{SK}_{\mathrm{v}}}$. Similarly, a pedestrian computes its tracing information $\mathrm{T}_{\mathrm{p}} = \mathrm{g}_3^{\mathcal{SK}_{\mathrm{p}}}$ where g_{i} represent random generator of $\mathbb{G}_{\mathrm{i}}$. Vehicle and pedestrian send $(\mathcal{PK}_{\mathrm{v}}, \mathcal{PK}_{\mathrm{p}}, \mathrm{T}_{\mathrm{v}}, \mathrm{T}_{\mathrm{p}})$ to $\mathcal{TC}$.

Step 2: $\mathcal{TC}$ performs authentication check by checking $e\left(\mathcal{PK}_v, \mathcal{PK}_p, g_2, g_3\right) = e(U_v, U_{p,} T_v, T_p)$. Upon success verification, $\mathcal{TC}$ generates a signature on $\mathcal{PK}_v$ and $\mathcal{PK}_p$. $\mathcal{TC}$ sends to $\mathcal{V}$ and $\mathcal{P}$ respectively. $\mathcal{TC}$ then stores $(\mathcal{PK}_v, \mathcal{PK}_p, T_v, T_p)$ into its local database.

Step 3: $\mathcal{V}$ runs a Zero-Knowledge Proof Protocol (ZKPP) denoted by $\mathcal{ZK}\{\mathcal{SK}_v | \mathcal{PK}_v = U_1^{\mathcal{SK}_v}\}$ with $\mathcal{RC}$. $\mathcal{RC}$ first verifies the signature on $\mathcal{PK}_v$ and $\mathcal{PK}_p$ to certify the legitimacy of the vehicle and pedestrian in the network. The $\mathcal{RC}$ has a key pair denoted by $(\mathcal{A}, \mathcal{Z}) = (e(\mathcal{Z}, g_2, g_3), \mathcal{Z})$. Then, $\mathcal{RC}$ validates $\mathcal{TC}$'s signature on $\mathcal{PK}_v$ and $\mathcal{PK}_p$. $\mathcal{RC}$ checks the ZKPP runs by $\mathcal{V}$ such that $\mathcal{ZK}\{\mathcal{SK}_v | \mathcal{PK}_v = U_1^{\mathcal{SK}_v}\}$ is valid and performs computation $K_1 = g_1^k$, $K_2 = Z(h_1 \mathcal{PK}_v)^{-k}$ and $K_p = Z(h_p \mathcal{PK}_p)^{-k}$ where $k \in \mathbb{Z}_p^*$. Upon success computation, $\mathcal{RC}$ distribute $K_v = (K_{1,} K_2)$ to legitimate vehicle and K_p to authorized pedestrian. A vehicle verifies that $e\left(K_{2,} g_2\right) e(K_{1,} h_2) e\left(K_1^{\mathcal{SK}_v}, U_2\right) = A$ to validate the signature. If the check holds, vehicle and pedestrian have successfully register to cloud and use K_v across the network as a group certificate. Vehicle can use its $\mathcal{SK}_v$ to generate signature on any safety message.

5.3 Message Broadcast

In this phase, a $\mathcal{V}$ generates a safety-related message and broadcasts it to neighbouring vehicles via RSUs. This is outlined as follows:

Step 4: $\mathcal{V}$ generates the message ($\mathcal{m}$) as follow:

$$\mathcal{m} = (MT, t_{stamp}, loc_{cur}, GID_v, ID_{RSU})$$

Message type is denoted as MT, t_{stamp} is the signature generation time to ensure message freshness, loc_{cur} is current position of the vehicle moving. Let GID_v be a group identity of the vehicle where it enable to distinguish which group corresponds to the vehicle. The real identity of RSU is denoted as ID_{RSU}.

Under the group signature scheme, a member of the group signs a message on behalf of the group. Signatures can be checked with regard to a specific public key group, but does not disclose the identity of the signatory. The group signature is composed of three parts as below:

- Distribute in a random way the group certificate to prove that the signatory is a lawful member of the group while protecting privacy on the network. $\mathcal{V}$ computes $\sigma_1 = K_1 g_1^s$, $\sigma_2 = K_2(h_1 \mathcal{PK}_v)^{-s}$ for a randomly chosen $s \in \mathbb{Z}_p^*$.

- Set up the public key of a group member in a random where, $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$ and produce a message link-identifier $\sigma_4 = H_1(m)^{\mathcal{SK}_v}$.

- Generate the group signature on m using private key, $\mathcal{SK}_v$ in $\sigma_3 = \sigma_1^{\mathcal{SK}_v}$ and $\sigma_4 = H_1(m)^{\mathcal{SK}_v}$. $\mathcal{V}$ executes zero knowledge proof to convince the verifier of a given statement's validity, without leaking any further information than the statement's validity to generate a group signature.

To generate a group signature, $\mathcal{V}$ performs the following computation:

- Randomly choses $r \leftarrow \mathbb{Z}_p^*$.

- Calculate assumptions $R_1 = H_1(m)^r$ and $R_2 = \sigma_1^r$.

- Obtain a challenge from the computed assumptions of R_1 and R_2 where $\sigma_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4||R_1||R_2)$.

- Response to the challenge with $\sigma_6 = r - \sigma_5^{\mathcal{SK}_v} \, mod \, p$ and output the group signature as $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_{6)}$ of m.

$\mathcal{V}$ broadcasts a message tuple, $\mathcal{M} = (m, \sigma)$. The message link-identifier, σ_4 that can only produce once by $\mathcal{V}$ for the same message. $\mathcal{V}$ then announce messages to authentication cloud, $\mathcal{AC}$ via RSU.

Step 5: RSU forward $\mathcal{M}$ to $\mathcal{AC}$ to evaluate the reliability of the safety messages. RSU rejects messages that included the same σ_4 as replay of σ_4 demonstrates that the same messages were signed by the same vehicle more than once. The $\mathcal{AC}$ then validates predefined number of messages reporting the same event.

5.4 Message verification

Upon receiving the message, cloud performs the following steps:

Step 6: For message verification:

$\mathcal{AC}$ checks $e(\sigma_{2,} g_{2,} g_3) e(\sigma_{1,} h_2, h_3) e(\sigma_3, U_2) = A$ in order to validate the group certificate. It then performs check on:

$$\sigma'_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4 \left|\left| H_1(m)^{\sigma^6} {\sigma_4}^{\sigma^5} \right|\right| {\sigma_1}^{\sigma^6} {\sigma_3}^{\sigma^5})$$

If the freshness of the message is preserved, $\mathcal{AC}$ considers a message to be reliable if and only if $\sigma'_5 = \sigma_5$. In addition, our protocol adopts flexible threshold authentication where $\mathcal{AC}$ measures the reliability of a message based on the influx of messages reporting similar event received.

Step 7: Upon success verification, $\mathcal{AC}$ forwards the safety message, $\mathcal{M}$ to nearby RSU.

Step 8: RSU broadcast the safety message $\mathcal{M}$ to $\mathcal{V}$ and $\mathcal{P}$ via RSU in the vicinity of the event reported.

Step 9: $\mathcal{V}$ and $\mathcal{P}$ validate the content of the message by checking the t_{stamp}. If t_{stamp} are valid and both checks for message verification hold, the safety message is considered reliable. To ensure the message is reliable and verified by $\mathcal{AC}, \mathcal{V}$ randomly choses s and computes $x = h(s)$ where x demonstrate the knowledge of s without disclosing it. $\mathcal{V}$ computes the challenge $f = (s, \mathcal{PK})_{\mathcal{AC}}$ and sends to $\mathcal{AC}$. Here, $\mathcal{PK}_{\mathcal{AC}}$ denotes the public key of $\mathcal{AC}$ and h is a one-way hash function. $\mathcal{AC}$ responds to the challenge by decrypting f to retrieve s' and computes $x' = h(s)'$ and terminate if $x' \neq x$ (implying $s' \neq s$). Otherwise, $\mathcal{AC}$ sends $s = s'$ to $\mathcal{V}$. Hence, $\mathcal{V}$ successfully authenticate $\mathcal{AC}$ upon verifying the received s agrees with that sent earlier.

5.5 Vehicle Traceability and Revocation

Step 10: $\mathcal{V}$ and $\mathcal{P}$ lodge a revocation report to the $\mathcal{TC}$ when experienced misbehaviour in the network.

Step 11: The $\mathcal{TC}$ validates the authenticity of $\mathcal{M}$ to revoke misbehaved $\mathcal{V}$. We note that $\mathcal{TC}$ holds some $\mathcal{PK}_{\mathcal{V}}$ trapdoor knowledge. For revocation and law enforcement purposes, the $\mathcal{TC}$ check its local database to link $\mathcal{PK}_{\mathcal{V}}$ with $\mathcal{V}'s$ identity. We adopt the revocation protocol from our previous work in [20] and refer the readers to [20] for in depth understanding of the revocation phase.

6. Security and Performance Evaluation

6.1 Security Analysis

In this section, we evaluate and discuss security issues and performance level of our proposed protocol. We compare our scheme with CLSS [15] and PPDAS [24] as both schemes are authenticated anonymous announcement protocol in IoV. The following security requirements are critical concerns to be met towards IoV deployment.

1) **Reliability**. The first two conditions of message reliability of are fulfilled in all aforementioned schemes. A secure digital signature technique is commonly used to achieve message authentication. Messages announced without modification is assured and the authenticity of the message is preserved. The necessity of user authenticity and data integrity is met in our protocol as message is signed using valid credentials issued by the cloud.

The scheme in [24] fulfil the third requirement of message trustworthiness by using reputation system to evaluate message reliability. However, it is not satisfied in [15], as no solution to evaluate message reliability was proposed. The property of threshold technique is not suitable to be adopted as the origin of the message in [15] is indistinguishable. In our work, we fulfil the requirement of threshold authentication property. We adopt the flexible threshold system which allows the cloud to determine the threshold depending on the message's content and location. For example, the threshold in a city is higher compared to the rural area, which is relative to traffic density.

Claim 1. *The proposed protocol is robust against Sybil attack and achieves the third requirement of message reliability.*

We consider a Sybil attack executed by an internal adversary. An external adversary is not considered, as they do not own a valid credential or direct access to the network thus pose less harms to other users in the network. Sybil attack occurs when an internal adversary generates multiple signatures and disguise as different vehicles in order to compromise the functionality of the IoV network.

Proof: Let an internal adversary be Ψ. We consider a scenario where Ψ generates two signatures on the same message and announce these messages. Upon receiving these messages, $\mathcal{AC}$ checks the message-link identifier, σ_4 to ensure that a legitimate vehicle in the network generates each message once. However, Ψ can be identified when the two signatures share the same component of

$$\sigma_4 = H_1(m)^{\mathcal{SK}_v}. \tag{1}$$

Hence, Ψ can be computationally related by evaluating the component of σ_4 on two messages reporting the same event. Therefore, our scheme provides the distinguishability of origin that supports threshold authentication and thus, achieve the requirement of message reliability.

Recall that, 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 the value of $\mathcal{SK}_V$ is undisclosed in (σ_3, σ_4). The $\mathcal{TC}$ uses the tracing information $T_v = g_2^{\mathcal{SK}_v}$ to identify the group member by checking

$$e\left(\mathcal{PK}_v, \mathcal{PK}_p, g_2, g_3\right) = e(U_v, U_p, T_v, T_p). \tag{2}$$

This enable Ψ to be traceable when the replay of σ_4 is recognized upon endorsing the same message more than once. Hence, the message will be discarded and thus, our protocol is robust against Sybil attack.

2) **Privacy**. We consider two elements of privacy, which are anonymity and unlinkability. In CLSS [15] and PPDAS [24], the requirement of privacy is achieved by the use of pseudonyms where it avoids linking the real identification of the vehicle to its source. Furthermore, different messages announced from an origin cannot be linked to each other. In our work, we satisfy the property of privacy.

Claim 2. *Our protocol protects the privacy of the originators against an internal adversary.*

Proof: Let an internal adversary be $\mathcal{B}$. Consider the following anonymity game. We generate key pair as depicted in our work and obtaining n key pairs $(\mathcal{PK}_{v_1}, \mathcal{SK}_{v_1})$,…, $(\mathcal{PK}_{v_n}, \mathcal{SK}_{v_n})$. The system parameters μ is forwarded to adversary $\mathcal{B}$ upon request where

$$\mu = \langle p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, g_3, e, h_1, h_2, h_{3,} U_1, U_v, U_{p,} H_1, H \rangle \tag{3}$$

We assume that the adversary $\mathcal{B}$ query the vehicle's secret key at index i, $1 \leq i \leq n$. We respond with key pair $(\mathcal{PK}_{v_i}, \mathcal{SK}_{v_i})$. We produce a valid signature σ_i on $\mathcal{M}$ using $\mathcal{SK}_{v_i}$ and forward σ_i to $\mathcal{B}$. The adversary $\mathcal{B}$ then generates a message $\mathcal{M}^*$. We randomly choose a bit $\mathscr{b} \in_{\mathcal{R}} \{0,1\}$ where $\mathscr{b}$ is unknown to us. We then compute a signature σ^* on $\mathcal{M}^*$ using $\mathcal{SK}_{v_{i_{\mathscr{b}}}}$. We send σ^* to $\mathcal{B}$. When $\mathcal{B}$ obtains the signature, $\mathcal{B}$ analyses the signature and outputs the guess of $\mathscr{b}$' of $\mathscr{b}$ where $\mathscr{b}' \in_{\mathcal{R}} \{0,1\}$. We declare failure and $\mathcal{B}$ wins the game, provided that $\mathcal{B}$ can guess the value of $\mathscr{b}' = \mathscr{b}$. This anonymity game defines the advantage of adversary $\mathcal{B}$ winning the game as equation (4), where Pr $[\mathscr{b}' = \mathscr{b}]$ represents the probability of $\mathscr{b}' = \mathscr{b}$

$$\Pr[\mathscr{b}' = \mathscr{b}] = \frac{1}{2} \tag{4}$$

The probability is taken over the coin tosses of adversary $\mathcal{B}$. Consequently, the adversary $\mathcal{B}$ is unable to exploit the randomized key generation and signing algorithm to win the anonymity game in polynomial time with a non-negligible probability. Hence, our protocol satisfies the privacy requirement.

3) **Accountability**. An entity performing some unlawful actions is traceable by the TP. Moreover, it must satisfy non-repudiation, that is, the assurance that they cannot deny to be the originator of the malicious message. When the malicious activity is proven true, the TP has evidence to revoke the vehicle off the network.

Claim 3. *Our protocol achieves all the accountability requirements.*

Proof: We fulfil the accountability requirements of traceability, non-repudiation and revocation in our scheme. The property of traceability is satisfied where the group signature allows the $\mathcal{TC}$ to reveal signature of a malicious vehicle. The identity of an adversary is traceable when the same component of σ_4 is recognized upon verifying the same message more than once and the proof runs similar to the proof in Claim 1. Non-repudiation is achieved since $\mathcal{AC}$ does not have access to the vehicle's secret key as the vehicle is the sole holder of the signing key, as illustrated in our scheme. Meanwhile, revocation is supported by the $\mathcal{TC}$ who maintains some trapdoor information to revoke dishonest vehicles. For an elaboration of the revocation technique, we refer the readers to our previous work in [20].

We prove that our security analysis completes the security requirements of message reliability, privacy and accountability in IoV network. **Table 2** presents a summary of the security requirements analysis. In our work, we successfully satisfy the conflicting security requirements of message reliability, privacy and accountability simultaneously which outperform [15, 24].

Table 2. Security Requirements in IoV

Security goal	**Security element**	**CLSS [15]**	**PPDAS [24]**	**Our work**
Reliability	Sender's authenticity	√	√	√
	Data integrity	√	√	√
	Message truthfulness	X	√	√

Privacy	Anonymity	√	√	√
	Unlinkability	√	√	√
Accountability	Traceability	√	√	√
	Non-repudiation	√	X	√
	Revocation	X	X	√

6.2 Performance Analysis

In this section, we evaluate the performance efficiency between our proposed protocol with CLSS [15] and PPDAS [24] as both schemes are anonymous authenticated announcement protocol in IoV. To provide a standard 80-bit security level, we set p a 160-bit long prime and the element in $\mathbb{G}_1$ to be 160 bits long by choosing an appropriate curve such as the National Institute of Standards and Technology (NIST) curve [32].

Communication cost. With respect to communication overhead, in our work, an announced message is composed of one payload, one time stamp, one group ID and one real identity of RSU. If we use 100 bytes, 2 bytes, 2 bytes and 1 bytes to represent a payload, a time stamp, a group ID and real identity of RSU respectively, then the length of vehicle-generated messages with 80-bit security level is computed as 100 + 2 + 128 + 2 + 1 = 233 bytes. In CLSS [15], the length of message is 640 bytes while in PPDAS [24], the message size is 849 bytes. Our scheme deploy group signature where the size of the signature is 128 bytes. Hence, our protocol efficiently achieve lower communication cost compared to [15, 24]. This is depicted in **Fig. 3**.

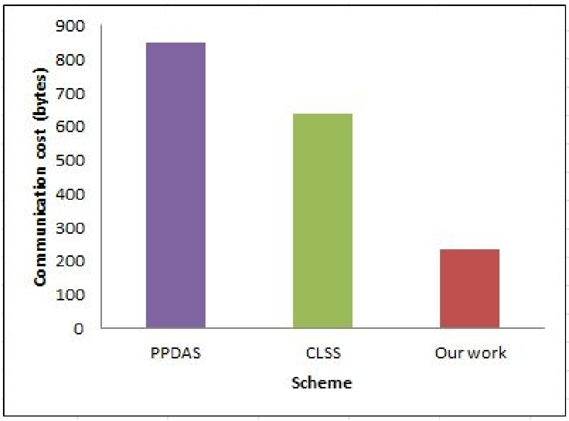

Fig. 3. The communication cost of our protocol compared with CLSS [15] and PPDAS [24]

Computational cost. We evaluate the computational cost of signature generation and verification in message broadcast. We consider the three most expensive operations, which are scalar multiplication in $\mathbb{G}_1$, exponentiation in $\mathbb{G}_T$ and pairing operation. We compare the computational cost between our scheme with [15] and [24] for $t = 1$. In this table, $k.\mathbb{G}_1$ indicates k scalar multiplications in $\mathbb{G}_1$, $r.P$ indicates r pairing operations. The signing operation in CLSS [15] requires $2.\mathbb{G}_1$ and the verification require $1.P + 3.\mathbb{G}_1$. Meanwhile, the PPDAS [24] requires $1.P + 1.\mathbb{G}_1$ for the signing operation, whereas the verification phase requires$1.P + 5.\mathbb{G}_1$. The signing procedure for our proposed protocol requires $6.\mathbb{G}_1$ and the verification requires $1.P + 4.\mathbb{G}_1$ operations. These findings are summarised in **Table 3**. We observe that the computational cost for our scheme is comparable with CLSS [15] and PPDAS [24] scheme.

Computation time. For $p = 160$ bits and $\mathbb{G}_1 = 161$ bits, one pairing evaluation and one scalar multiplication in $\mathbb{G}_1$ takes 4.5 ms and 0.6 ms respectively [2]. Using this information, we calculate the computation time of operations tabulated in the computational cost column of **Table 3**. For instance, the 'sign' operation in our work takes $6.\mathbb{G}_1 = 6(0.6)$ to obtain 3.6 ms. Similarly for the 'verify' operation, for $1.P + 4.\mathbb{G}_1 = 1.(4.5) + 4.(0.6)$ to obtain 6.9 ms. We present the rest of the result in the computation time column of **Table 3**.

From the discussion above, we conclude that our work achieves the most efficient communication cost than [15, 24]. Meanwhile, in terms of computation cost and time, our work is more efficient than PPDAS [24] and achieve comparable performance to CLSS [15]. Furthermore, we satisfy all security requirements needed for a success deployment of an announcement protocol in IoV compared to [15, 24]. **Table 2** and **Table 3** summarize the overall performance.

Table 3. Comparison of Performance Analysis

Scheme	Communication cost	Computational cost		Computation time	
		Sign	Verify	Sign (ms)	Verify (ms)
CLSS [15]	640 Bytes	$2.\mathbb{G}_1$	$1.P + 3.\mathbb{G}_1$	1.2	6.3
PPDAS [24]	849 Bytes	$1.P + 1.\mathbb{G}_1$	$1.P + 5.\mathbb{G}_1$	5.1	7.5
Our work	233 Bytes	$6.\mathbb{G}_1$	$1.P + 4.\mathbb{G}_1$	3.6	6.9

6.3 Simulation

The network simulator NS-2.35 was used. Our simulation analyses are conducted based on the V2V and V2P communication. We implement IEEE 802.11a as the wireless network. We note that this wireless network offering service same as 5G network protocol. We evaluated two major performance metrics for V2V communication, denoted as average message delay (MD_v) and average message loss ratio (ML_v). We also analysed average message delay (MD_v) for V2P communication. We assume the vehicular nodes and pedestrian are distributed at random. In order to assess our performance metric, we formulated in such a way:

$$MD_v = \frac{N_v \times M_{sent} \times T_{sign}}{M_{received}}$$

$$ML_v = \frac{(N_v - M_{received}) \times T_{verify}}{N_c \times N_v}$$

$$MD_p = \frac{N_p \times N_v \times (T_{sign} + T_{verify})}{N_p}$$

where N_v, N_c, N_p is number of vehicle, cloud and pedestrian respectively. Meanwhile, M_{sent} is amount of message sent and $M_{received}$ known as amount of message received. Total signature time denoted as T_{sign} and total verification time symbolize as T_{verify}. The simulation design setting for this scheme is as follows:

Table 4. Simulation Parameters

Parameters	**Value**
Mobility Model	Ad hoc On-Demand Distance Vector (AODV)
Simulation region	2 km x 2 km
Simulation time	30 min
No of vehicles	20-100
No of pedestrian	5-25
Speed of vehicles	20-108 km/h
Speed of pedestrian	5 km/h
Data rate	6 Mbps
Messaging frequency	10 Message/s, 20 Message/s

The simulation results are shown in **Fig. 4** and **Fig. 5** for V2V communication. In this experiment, we set our threshold at $(t) = 5$ where (t) indicates trustworthiness of messages. The trustworthiness of message can be illustrated as a vehicle observing the same event in the vicinity and agrees with the broadcasted safety message.

Fig. 4 shows the simulation result of average message delay with respect to number of vehicles. A higher average of message delay implies that a lower number of vehicles can utilize the verified message, hence affect the driving efficiency. We assume each vehicle broadcast one message. We observe that our work yields the lowest message delay followed by CLSS [15] and PPDAS [24] schemes. We consider this is natural because a higher number of vehicles in the vicinity may receive a higher number of verified of the same message up to the predefined threshold. This proves that our proposed protocol has advantage over other schemes.

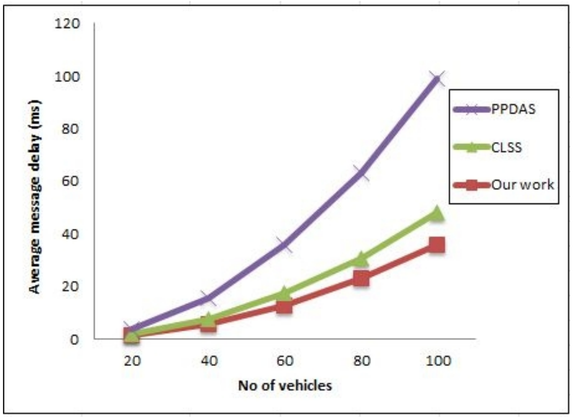

Fig. 4. The relationship between average message delay and number of vehicles

Fig. 5 shows the simulation result of average message loss ratio with respect to number of vehicles. The average message loss demonstrates the protocol's validity and feasibility. For a given threshold, we observe that, the average message loss increases as the number of vehicle increase. We discover that this feature is triggered by a large number of messages being lost because the bulk of the message is sent repeatedly due to heavy traffic. In terms of message loss, our scheme apparently comparable and better than CLSS [15] and PPDAS [24] schemes.

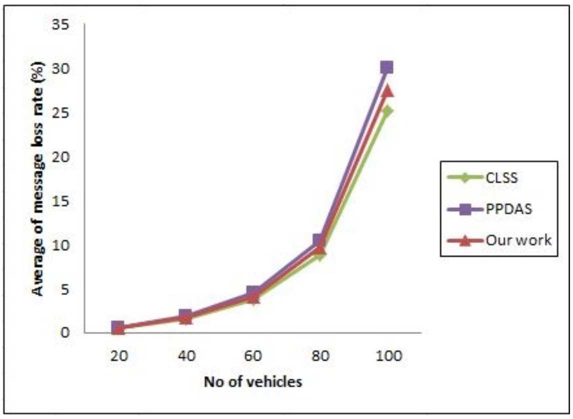

Fig. 5. The relationship between average message loss ratio and number of vehicles

Meanwhile, for V2P communication, we observe the simulation result of average message delay against number of pedestrian as in **Fig. 6**. As we can see, the rate of average message delays grows almost linearly to number of pedestrian in simulation area. This functionality ensures that our protocol is acceptable to different traffic situations and does not significantly degrade its performance in the case of a large number of vehicles.

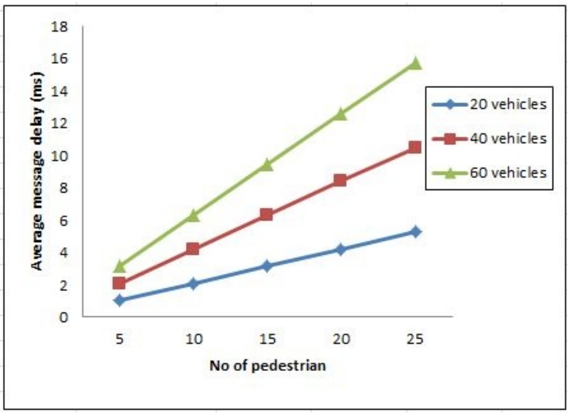

Fig. 6. The relationship between average message delay and number of pedestrian

7. Conclusion

In this paper, we have presented a secure and efficient announcement protocol for IoV network where the underlying cryptographic primitive is based on group signature. Our comprehensive construction of generic abstraction may assist to provide guidelines to design future announcement protocol based on group signatures in IoV network. As far as we are aware, this is the first generic abstraction for announcement protocol using group signature for IoV in the literature. We designed a new group signature announcement protocol based on our generic abstraction. We have demonstrated that our protocol efficiently addresses the conflicting security requirements of reliability, privacy and accountability simultaneously. Implementation of our work on NS-2.35 simulator proves the practicality and applicability of our protocol in real world deployment.

For future work, extending the current scheme would be of interest where a pedestrian could also announce the safety-related messages without compromising the security requirements. Other possible direction is to explore different cryptographic techniques to design anonymous authenticated announcement protocols in IoV.

References

[1] WHO. Global status report on road safety, 2015. Available Online: 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, 2013. 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] J. Cui, W. Xu, H. Zhong, J. Zhang, Y. Xu, and L. Liu, “Privacy preserving authentication using a double pseudonym for internet of vehicles,” *Sensors*, vol. 18, no. 5, p. 1453, 2018. 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] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, “Systematic literature review on internet of vehicles communication security,” *Int. J. of Distri. Sensors Netw.*, vol. 14, no. 12, 2018. Article(CrossRef Link)

[11] J. Joy and M. Gerla, “Internet of vehicles and autonomous connected car - privacy and security issues,” in *Proc. of 26th Int. Conf. on Comp. Commun. and Netw.*, pp. 1-9, 2017. Article(CrossRef Link)

[12] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, “Security and privacy in the internet of vehicles,” in *Proc. of Int. Conf. on Identification Information and Knowledge in the IoT*, pp. 116-121, 2015. Article(CrossRef Link)

[13] J. Cui, W. Xu, H. Zhong, J. Zhang, Y. Xu, and L. Liu, “Privacy preserving authentication using a double pseudonym for internet of vehicles,” *Sensors*, vol. 18, no. 5, p. 1453, 2018. Article(CrossRef Link)

[14] J. Kang, R. Yu, X. Huang, and Y. Zhang, “Privacy preserved pseudonym scheme for fog computing supported internet of vehicles,” *IEEE Trans. Intel. Transp. Sys.*, vol. 19, no. 8, pp. 2627-2637, 2018. Article(CrossRef Link)

[15] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, “An efficient anonymous authentication scheme for internet of vehicles,” in *Proc. of 2018 IEEE Int. Conf. on Commun.*, pp. 1–6, May 20-24, 2018. Article(CrossRef Link)

[16] R. Sahbi, S. Ghanemi, and R. Djouani, "A network model for internet of vehicles based on SDN and cloud computing," in *Proc of 6th Int. Conf. on Wireless Networks and Mobile Commun., WINCOM 2018*, pp. 1-4, 2018. Article(CrossRef Link)

[17] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on internet of vehicles communication security," *Int. J. of Distr. Sensor Netw.*, vol. 14, no. 12, pp. 1-21, 2018. Article(CrossRef Link)

[18] 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)

[19] 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)

[20] N. F. M. Shari, A. Malip and W. A. M. Othman, "Revocation protocol for group signatures in VANETs: A Secure Construction," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 1, pp. 299-322, 2020. Article(CrossRef Link)

[21] R. Argawal, S. S. Pranay, K. Rachana, and H. P. Sultana, "Identity based security scheme in internet of vehicles," *Smart Intel. Comp. and App., Smart Innovation, Sys. and Tech.*, vol. 104, pp.515-523, 2019. Article(CrossRef Link)

[22] Chen, B. Xiang, Y. Liu, and K. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047-12057, 2019. Article(CrossRef Link)

[23] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," *IEEE IoT J.*, vol. 4, no. 2, pp. 601-610, 2017. Article(CrossRef Link)

[24] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Systems*, vol. 18, no. 10, pp. 2740-2749, 2017. Article(CrossRef Link)

[25] H. Vasudev and D. Das, "An efficient authentication and secure vehicle to vehicle communications in an IoV," in *Proc.of 89th IEEE Veh. Tech. Conf., VTC Spring 2019*, pp. 1-5, 2019. Article(CrossRef Link)

[26] V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE Trans. Veh. Tech.*, vol. 58, no. 4, pp. 1876-1886, 2009. Article(CrossRef Link)

[27] G. Kounga, T. Walter, and S. Lachmund, "Proving reliability of anonymous information in vehicular ad hoc networks," *IEEE Trans. Veh. Tech.*, vol. 58, no. 6, pp. 2977-2989, 2009. Article(CrossRef Link)

[28] M. Raya, A. Aziz, and J. Hubaux, "Efficient secure aggregation in vehicular ad hoc networks," in *Proc. of the Third Int. Workshop on VANET, VANET 2006*, pp. 67-75, Sept 29, 2006. Article(CrossRef Link)

[29] M. A. Ferrag, L. A. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. of Netw. and Comp. App.*, vol. 101, pp. 55-82, 2018. Article(CrossRef Link)

[30] K. M. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETS," *IEEE Computer Society Digital Library*, vol. 1, pp. 304-313, 2007. Article(CrossRef Link)

[31] An introduction to pairing-based cryptography, Recent trends in cryptography, American Mathematical Society, 2009.

[32] P. Mell and T. Grance, "The NIST definition of cloud computing," *Special Publication*, vol. 800, p. 145, 2011.

[33] N. Bermad, S. Zemmoudj, and M. Omar, "Context-aware negotiation, reputation and priority traffic light management protocols for VANET-based smart cities," *Telecom. Syst.*, vol. 72, no. 1, pp. 131-153, 2019. Article(CrossRef Link)

Nur Afiqah Suzelan Amir received the B.Sc. (first class) degree from the University of Technology Mara, Malaysia at 2016. She is currently pursuing the M.Sc. degree in Mathematics from the University of Malaya, Malaysia. Her current research interests are cryptographic protocols, wireless and network security.

Amizah Malip received the M.Sc. degree in mathematics of cryptography and communications and Ph.D. degree in information security, both from the Royal Holloway, University of London, UK. She is currently a Senior Lecturer with the Institute of Mathematical Sciences in the University of Malaya, Malaysia. Her main research interests include privacy, network security, vehicular communications and cryptographic applications.

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.