Vehicle Identity Anonymity Framework with Accountability for VANET Environment

Nai-Wei Lo[1], Chi-Ying Chuang[1], Jia-Ning Luo[2], Chong-Long Yang[1]*

[1] Department of Information Management, National Taiwan University of Science and Technology, Taiwan
[2] Department of Computer Science and Information Engineering, National Defense University, Taiwan
nwlo@cs.ntust.edu.tw, d10916005@mail.ntust.edu.tw, deer@ccit.ndu.edu.tw, m10709112@mail.ntust.edu.tw

Abstract

In recent years, there has been rapid development in vehicle safety technology, with the emergence of various active safety systems including blind spot information systems, adaptive cruise control, and front collision warning systems. Simultaneously, car manufacturers and technology companies are actively exploring technologies in the realm of autonomous driving. To facilitate such applications, vehicles are required to communicate with each other, exchanging vital information such as position, speed, and acceleration.

However, this exchange of information poses a potential risk of drivers' personal data being compromised. For safety purposes, vehicles must undergo appropriate authentication before engaging in communication with other vehicles. Ensuring this authentication process maintains the anonymity of the vehicles is crucial. Yet, striking a balance between protecting vehicle anonymity and enabling vehicle identification when necessary remains a challenging issue.

This paper introduces a multi-tier Vehicular Ad-Hoc Network (VANET) framework designed to uphold the conditional anonymity and traceability of vehicles. The implementation of a group signature mechanism facilitates anonymous authentication, thereby enabling the realization of conditional anonymity and traceability. Moreover, comprehensive simulations and security analyses were conducted to validate the effectiveness of the proposed framework, demonstrating its efficiency while incorporating robust safety considerations.

Keywords: Vehicular ad-hoc network, Vehicle to Infrastructure, Group signature, Pseudonym

1 Introduction

The Vehicular Ad-Hoc Network (VANET) represents a distinct variant of the Mobile Ad-Hoc Network (MANET). Within VANET, nodes are facilitated by vehicles traversing diverse environments, including highways, rural roads, and urban thoroughfares. These nodes are obligated to adhere to traffic regulations, encompassing compliance with traffic signs, speed limits, and road layouts, necessitating adherence to numerous restrictions, thus precluding unrestricted actions. Furthermore, in contrast to MANET, VANET encounters relatively limited device computing capabilities, storage capacities, and power-related constraints. Within the VANET, two distinct communication scenarios are delineated:

1. A collection of neighboring vehicles on the road establishes a transient network to relay crucial messages among themselves. All vehicles within this network engage in mutual communication and message exchange. This mode of communication is commonly referred to as Vehicle-to-Vehicle (V2V) or Inter-Vehicle Communication.
2. Alongside V2V communication, interaction with various Roadside Units (RSUs) also takes place, denoted as Vehicle-to-Infrastructure (V2I) communication.

Previously, owing to multiple factors like network limitations, device computing capabilities, and power constraints, the utilization of Internet of Things (IoT) devices primarily centered around sensing functions. However, with the recent advancements in wireless communication technology and service network infrastructure, there has been a rapid progression in Intelligent Transportation Systems (ITS). The expansion and implementation of ITS encompass a wide array of functionalities, including autonomous driving, public transportation management, intelligent ticketing systems, and traffic safety control. VANET assumes a critical role within the ITS domain. V2V and V2I communication constitute essential components of ITS. As vehicles traverse, they establish communication with the external environment through wireless network connectivity, availing external services and resources. These services include transmitting messages to nearby vehicles, receiving multimedia data from other vehicles, and accessing diverse service offerings.

The initial application of VANET primarily serves to furnish valuable information to drivers, aiding them in making informed judgments about road conditions [1]. Moreover, VANET facilitates road safety enhancement through seamless integration of V2V and V2I communications. Achieving the aforementioned objectives necessitates the transmission of messages via wireless communication and networks. Various wireless communication standards are available for this purpose, such as Dedicated Short-Range Communication (DSRC), WiFi, 4G/5G, and others. These protocols can be interconnected via Transmission Control Protocol/Internet Protocol (TCP/IP), Open Service Gateway initiative (OSGi),

*Corresponding Author: Jia-Ning Luo; E-mail: deer@ccit.ndu.edu.tw

DOI: 10.53106/160792642024032502009

Universal Plug and Play (uPnP), and Hypertext Transfer Protocol (HTTP) for the web, among other protocols.

According to the yearly statistics of police administration in Taiwan [2], the number of car accidents that occurred in Taiwan in 2021 was 358,221, of which category A1 accounted for 1806, and category A2 accounted for 356,415. Category A1 refers to accidents that cause people to die within 24 hours, and category A2 refers to accidents that cause people injury or death after 24 hours.

The procedure for managing traffic accidents in Taiwan includes the following steps:

1. Immediately stop to inspect personal well-being and assess the vehicle's damage. Activate the hazard flashers and position a triangular warning sign 30 to 100 meters behind the vehicle, considering the speed and road conditions, to prevent potential collisions from rear-approaching vehicles.
2. In the event of any injuries, dial 119 to request an ambulance for transportation to the hospital. Subsequently, contact 110 to report the incident to the police.
3. Prior to the arrival of the law enforcement officers, ensure the preservation of the accident scene for the collection of evidence. Take photographs of the vehicle's front, back, left, and right sides. Cooperate with the police by providing supplementary information and notes.

In the event of a traffic accident, the urgency and chaos of the situation can impede the immediate implementation of the aforementioned steps or any other rescue efforts. This delay may potentially hinder prompt assistance, leading to difficulties in escape or the occurrence of hit-and-run incidents.

To solve the above problems, the European Union has introduced an e-call system. Through the integration of automobiles and wireless communication, the e-call system stands out as one of the most distinctive and practical applications. The fundamental concept underlying e-call involves the installation of a device in each vehicle, utilizing the Global Positioning System (GPS) to acquire the car's precise location information. In the event of an accident, the system's sensor automatically triggers an alarm, or the user manually initiates an emergency call for assistance.

When establishing a voice call, the e-call system transmits critical data to the Public Safety Answering Point (PSAP) as a Minimum Data Set (MSD). This dataset includes the vehicle's location, driving direction, license plate number, vehicle type, and the count of passengers. Such transmission enables the rescue center to pinpoint the accident site and organize immediate rescue operations swiftly. The primary objective of the e-call system revolves around expediting post-accident rescue efforts.

According to statistics results, from 2011 to 2015, there were 28,266 hit-and-run cases in Taipei City alone [3]. When a hit-and-run accident occurs, the police must find the cause, assist the injured to leave the scene for treatment, maintain road traffic conditions, and restore the road to unblocked. If the prisoner escapes at this time, the police must chase a hit-and-run driver when the road has been blocked, which is likely to cause other traffic accidents and cause more casualties.

In the VANET architecture, each vehicle must be equipped with an On-Board Unit (OBU). This component will publish beacon messages known as Cooperate Awareness Messages (CAMs) at a frequency of 1-10Hz. Beacon messages will be based on information related to the vehicle, including the location of the vehicle, driving speed, driving direction, and information about neighboring vehicles. Each vehicle can generate a so-called Local Dynamic Map (LDM) through the beacon messages sent by the surrounding vehicles so that the vehicle can know the traffic conditions nearby at any time. LDM is an environmental database maintained by each vehicle. Specific events, such as emergency brakes of preceding vehicles or road construction, can be broadcast through the Decentralized Environmental Notification Message (DENM), which uses multi-hop communication to expand spatial coverage. For example, notifying that an accident has occurred in front of surrounding vehicles or that a traffic jam on the road ahead is over. The RSU installed along the road can support information dissemination. For example, at an intersection, it can communicate with the infrastructure.

Because many applications of VANET are directly related to driving safety. Each vehicle will always be equipped with OBU and many sensors to sense changes in the surrounding environment and use wireless communication to communicate with other vehicles to improve cooperation and coordination. Vehicles participating in the network are broadcast beacon messages containing vehicle information all the time. This action may endanger the privacy of the driver, and an aggressive attacker can use this information to obtain the detailed trajectory of the vehicle. Therefore, the prevention of vehicle tracking and attacks that may leak the identity of the vehicle or driver must be taken seriously.

According to the EU's data protection law, the beacon messages should be treated as personal data [4]. Therefore, it is very important to ensure the safety of communication between vehicles and other devices, whether it is other vehicles or roadside facilities. Furthermore, because vehicles are closely related to people's lives, interested people can get other information through them. In addition to communication security issues, privacy-related issues also need to be explored.

To prevent vehicle tracking and thwart attacks aimed at uncovering the vehicle or driver's identity, thereby preserving privacy, Gerlach introduced the foundational approach to privacy protection in V2V in 2006 [5]. This approach involves the removal of all vehicle or driver identifiers from messages and certificates, substituting them with an abstract identifier assigned to the vehicle, alongside an embedded pseudonym within the certificate.

Nevertheless, in the context of vehicle-to-vehicle communication, the use of static pseudonyms alone is inadequate [6]. Adversaries still possess the capability to identify and track individual vehicles by analyzing the temporal patterns of messages. The broadcasted messages from vehicles often exhibit repetitive and foreseeable patterns attributable to specific drivers or vehicles. To address this concern, employing a set of pseudonyms rather than a single pseudonym proves to be a more effective approach.

This strategy involves the periodic rotation of pseudonyms, wherein a vehicle uses a specific pseudonym for a limited duration before transitioning to another pseudonym.

While leveraging pseudonyms to maintain anonymity, it is imperative for law enforcement agencies or other trusted third parties responsible for assigning vehicle pseudonyms to establish a robust connection between the vehicles and the pseudonyms. For instance, this can be achieved through the utilization of recorded data from the accident site for vehicle identification purposes.

This paper presents a framework designed to achieve conditional privacy and traceability by integrating group signatures, hierarchical deterministic pseudonyms, and V2I communication. When a vehicle is operating within the bounds of the law, its anonymity is guaranteed. However, in the event of unlawful activity, the vehicle can still be traced without compromising anonymity. The vehicle's anonymity is upheld through a robust security mechanism, with periodic changes of pseudonyms to deter identification and tracking by potential malicious users or third parties.

Even if an attacker intercepts the data transmitted by the user, they cannot ascertain the vehicle's location from the intercepted data. In the case of a vehicular accident, the affected vehicle forwards the pseudonym of the offending vehicle to a regional trusted third party, known as the Local Trust Authority, for investigation. Subsequently, the Local Trust Authority shares the pseudonym and group signature with a TA for further scrutiny. The TA employs hierarchical deterministic techniques to authenticate pseudonyms and seeds. After confirming the veracity of the vehicle's actions, the TA can decide whether to disclose the true vehicle ID or continue tracking it anonymously.

The paper is organized as follows: The initial section provides an overview of the research background, motivation, and contributions. Section 2 presents the technologies utilized in this study. Section 3 contains a comprehensive review of prior research in related fields, serving as a point of reference for this paper's research. Section 4 defines the assumptions, scenarios, framework architecture, and the proposed framework encompasses. Section 5 encompasses the configuration of the experimental environment and diverse analyses conducted for this framework. The concluding section offers a summary and outlines potential avenues for future research.

2 Preliminaries

The most renowned application of Hierarchical Deterministic technology is Bitcoin's Hierarchical Deterministic Wallet (HD Wallet). The advent of the HD Wallet is rooted in the recommendation within the Bitcoin White Paper for clients to utilize randomly generated keys, with a new key to be employed after each transaction. To obviate the necessity of backing up the key after every single transaction, Bitcoin Improvement Proposal 32 (BIP32) [7] introduced the concept of the HD Wallet, serving as the fundamental proposition for this wallet type. Bitcoin Improvement Proposals 39 (BIP39) [8] and Bitcoin Improvement Proposals 44 (BIP44) [9] collectively delineate the current standard of the HD Wallet widely in use.

This section provides an introduction to the foundational knowledge underpinning this paper and explores relevant literature. The initial segment outlines the concept and attributes of the group signature. The subsequent segment offers an overview of Bitcoin, particularly pertaining to BIP32 and BIP39 within the Hierarchical Deterministic Wallet framework. Finally, the section introduces the Elliptic Curve Diffie-Hellman Ephemeral.

2.1 Group Signature

The concept of group signature was initially introduced by Chaum and Heyst in 1991, aiming to utilize group-based authentication to safeguard the signer's privacy while ensuring authentication [10]. The group signature concept embodies the following notion: all group members can sign on behalf of the entire group, with the resulting signature being verifiable using the group public key. In essence, signatures signed by any member within the same group are indistinguishable from the signature verifier. The verifier cannot ascertain the signer's identity but can only determine their association with the group, thus ensuring the signer's anonymity.

However, within the group signature scheme, a trusted third party is the group manager. In instances where group members begin to engage in malicious activities and exploit the anonymity provided by the group signature scheme, the group manager holds the capability to revoke the anonymity conferred by the group signature scheme and disclose the signer's identity. We can divide a complete group signature scheme into four steps:

1. System setup
2. Signature generation
3. Signature verification
4. Opening procedure

A group signature system typically has two roles: the group manager and the group members. The group manager's responsibilities include initiating the group and managing the enrollment of group members. During group initialization, the group manager defines the group parameters and generates the group public key along with the manager's secret key. Following this process, the group manager utilizes the group parameters and their secret key to add individuals seeking to join the group, issuing a member secret key enabling them to sign signatures.

Each group member possesses only their respective member's secret key and can use it to sign messages. Any verifier aiming to authenticate the signature can utilize the group's public key to verify the group signature's validity. Furthermore, the group manager holds the capability to employ their own group secret key to unveil the group signature, consequently identifying the member within the group who signed the signature.

In contrast to typical digital signatures, group signatures aim to achieve two key security objectives:

1. Unforgeability: Only members belonging to the group possess the capability to produce a valid group signature on behalf of the group.
2. Privacy: Group signatures necessitate solely the group manager's awareness of the specific group

member who signed the signature, thereby ensuring the confidentiality of the members.

In the group signature scheme, the authority held by the group manager underscores the need for robust security measures, ensuring the safeguarding of both the group members and the mechanism's role. A fundamental purpose of the group signature is to enable verifiers to authenticate signatures even when user identities remain anonymous, guaranteeing that the signature indeed corresponds to a group member. One of its most prevalent applications is the concealment of organizational structures. Employees can use the group signature scheme to shield their personal information when engaging in various company-related activities, such as contract signing, news dissemination, or commercial transactions. This scheme ensures that employees' personal details remain undisclosed, thereby upholding their privacy.

Nevertheless, in cases where employees engage in actions detrimental to the company, such as deceiving consumers or conducting transactions under the company's name, the disclosure mechanism can be utilized by the company to unveil the employees' personal information, consequently safeguarding the company's interests.

2.2 Hierarchical Deterministic Wallet

In the Bitcon [11] Improvement Proposal 32 (BIP32) [7], the initial step of the HD Wallet involves selecting specific words from the designated wordlist to create the mnemonic code in line with the specifications of BIP39. Subsequently, the mnemonic sentence utilizes the Password-Based Key Derivation Function 2 (PBKDF2) to generate the seed. This key derivation function serves to slow down the derivation process. All keys are generated from this seed. Initially, the seed utilizes HMAC-SHA 512 to produce a 512-bit value, which is then split into a left half of 256 bits, known as the master key, and a right half of 256 bits, referred to as the master chain code.

An index is added alongside the key and chain code when generating a key. In BIP32, the index size is 32 bits, allowing each key to generate 2^{32} sub-keys. The master key can generate multiple child keys and child chain codes at the subsequent level, while the child keys can further generate grandchild keys and grandchild chain codes, resulting in the formation of a key tree, as depicted in Figure 1.

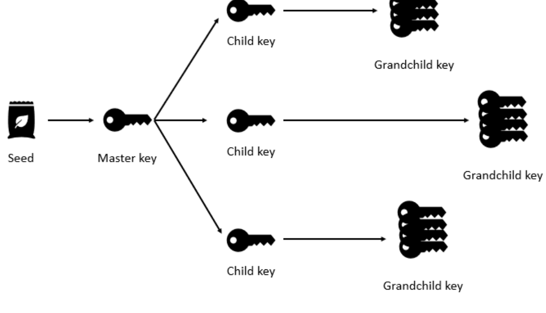


Figure 1. Key structure of HD wallet

This architecture's primary advantage lies in its convenience when clients frequently update their keys. With the seed, users can effortlessly generate the required key belonging to a specific layer and index, eliminating the need to store individual keys. However, this convenience is also the principal risk, as the exposure of the seed to the public sphere implies the potential compromise of all the keys derived from it.

2.3 Elliptic Curve Diffie-Hellman Ephemeral

The Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) represents a key agreement mechanism that integrates the Elliptic Curve Cryptography (ECC) algorithm with the Discrete Logarithm Problem (DLP). This mechanism enables two parties to establish a secure channel through an insecure medium without any prior knowledge. ECDHE operates as a temporary mode of the Elliptic Curve Diffie-Hellman (ECDH). Upon the initiation of each secure channel establishment, both parties generate distinct keys.

Unlike ECDH, where one party persists in using the same key, ECDHE guarantees forward secrecy by generating new keys for each session. This property ensures that even if one session key is compromised, subsequent keys remain secure, bolstering the overall security of the communication channel.

The procedure for ECDHE unfolds as follows, assuming two individuals, Alice and Bob, intend to securely exchange messages:

1. Alice and Bob select the same elliptic curve and obtain the base point G.
2. Alice generates her own private key a and calculates the public key $a \cdot \mathrm{G}$ via the elliptic curve cryptography.
3. Bob generates her own private key b and calculates the public key $b \cdot \mathrm{G}$ via the elliptic curve cryptography.
4. Alice and Bob exchange public keys through the insecure channel.
5. After obtaining Bob's public key $b \cdot \mathrm{G}$, Alice calculates $S_a = a \cdot (b \cdot \mathrm{G})$.
6. After obtaining Alice's public key $a \cdot \mathrm{G}$, Bob calculates $S_b = b \cdot (a \cdot \mathrm{G})$.
7. $S_a = S_b$ is the shared secret of Alice and Bob.

After completing the above steps, Alice and Bob can use the shared secret for Advanced Encryption Standard (AES) encryption to establish a secure channel.

3 Literature Review

In previous VANET research, the proposed pseudonym mechanisms can be broadly categorized into five groups based on different implementation mechanisms: PKI-oriented schemes, identity-based schemes, group signature schemes, symmetric cryptography schemes, and mix-zone related schemes.

3.1 PKI-oriented Schemes

This scheme employs Asymmetric Cryptography for communication. It involves preloading one or a group of distinct public key certificates along with their corresponding key pairs onto the vehicle, enabling communication through the use of asymmetric cryptography. These certificates do not contain any information that can be directly associated with the actual driver or the vehicle owner, effectively operating as pseudonyms. When receiving messages, the message recipient utilizes this certificate to verify the received message without gaining knowledge about the identity of the message sender.

Eckhoff et al. [12] introduced a time-slotted pseudonym pool approach, wherein each vehicle maintains its own pool of pseudonyms. These pseudonyms are rotated at predetermined intervals, with the length of the time slot determining the frequency of pseudonym changes. This strategy ensures that vehicles can autonomously update their pseudonyms without relying on any external third party, allowing them to maintain a valid pseudonym consistently.

On the other hand, Freudiger et al. [13] proposed a user-centric model for calculating the location privacy of vehicles in real time. They utilized Game Theory to develop a pseudonym replacement strategy for each mobile node. By analyzing scenarios with complete or incomplete information involving multiple players, they identified a balanced strategy for each node. This balancing strategy aids in finding the optimal approach for preserving privacy, even within a non-cooperative environment.

3.2 Identity-based Schemes

The Identity-based cryptography scheme utilizes a public key as the user's identifier and derives the corresponding private key from this identifier. In 2012, Lu et al. [14] introduced an authentication framework employing an ID-based online/offline signature (IBOOS) and an ID-based signature (IBS). The IBOOS method divides the signing process into online and offline stages, resulting in a notably faster authentication process compared to traditional Identity-based schemes.

In Zhang et al.'s solution [15], all vehicles utilize short-term pseudonyms for communication instead of certificates. These short-term pseudonyms are generated based on vehicle clock synchronization to facilitate the process of identity-based signature generation.

In addition to the aforementioned approach, Zhang et al. [16] proposed the Distributed Aggregate Privacy-Preserving Authentication (DAPPA) in 2017, based on MTA-OTIBAS (Multi-TA Offline/Online Identity-Based Aggregate Signature) and multiplicative secret sharing (MSS). The DAPPA scheme involves a root TA, lower-level TA (held by RSUs), and vehicles. Each RSU possesses a key pair usable within a restricted timeframe. Upon entering an RSU's jurisdiction, a vehicle undergoes registration with the RSU. Upon successful verification, the RSU provides the vehicle with a share of the restricted key and a defined time limit. The vehicle, upon receiving the share, can locally generate a one-time pseudonym key pair using the share and MSS.

3.3 Group Signature-based Schemes

Liu et al. proposed a scheme [17], that divides vehicles into two categories, protects private vehicle messages with a group signature scheme to provide security and privacy, and uses identity-based signatures for public vehicles and RSUs to reduce the management burden of keys and certificates.

The scheme of Shao et al. [18] proposed a decentralized group model and combined group signatures with an authentication threshold. In Shao's system model, vehicles within the communication range of the same RSU will obtain a group certificate to communicate with other vehicles in the same range. In addition, based on threshold authentication, OBU only receives messages with a certain number of valid signatures.

Yu et al. proposed the concept of mixgroup in their scheme [19]. They observed that most of the vehicles would pass through their respective social spots and encounter most of the vehicles they would encounter in a day. Therefore, they combined the social spot around the global social spot into a group region. When the vehicle enters this area, it will start to use the group signature for secure communication. In addition, the group leader of the area will give the vehicle a group of temporary pseudonyms, and the communication in the area will use these temporary pseudonyms. A temporary pseudonym will be used when a vehicle wants to exchange pseudonyms with other vehicles in the area.

3.4 Symmetric Cryptography-based Scheme

In the part of authentication, symmetric cryptography is not as flexible as asymmetric cryptography, but it can provide excellent computing and communication capabilities. In general, symmetric cryptography uses HMAC for message verification. The message sender first hashes the message and the symmetric key, and the receiver can only use the same steps and the same key to confirm whether the message sender is legitimate. But while providing lower computing time, it also lost accountability.

Xi et al. proposed a scheme that uses a random key pool to protect the privacy of users in 2007 [20]. First, all valid keys will form a key pool, and then each participant will randomly select a set of key sets from the pool. Under the correct circumstances, each key will be shared by a group of unspecified members. Therefore, when a participant uses a group of vehicle-shared keys as a key for identity verification, the authenticating party will not be able to identify the identity by the key.

In 2016, Vijayakumar et al. proposed a dual key management technique using the Chinese Remainder Theorem (CRT) [21]. TA first divides users into Primary Users (PUs) and Secondary Users (SUs). Further, TA directly provides service for PUs, SUs directly get service from Pus, and TA generates two different keys for different communication, preventing malicious vehicles from being mixed into legitimate vehicles or the entire VANET through dual authentication and key management.

3.5 Mix-zone-based Schemes

The Mix-zone mechanism is a branch of the pseudonym mechanism, which is to provide unlinkability between the old and new pseudonyms. Mix-zone refers to a method in which k users enter a specific area in different orders to change their pseudonyms and leave the area in different ways to provide pseudonym unlinkability.

Freudiger et al. [13] proposed a user-centric model of location privacy to calculate the location privacy of vehicles at any time and used game theory to formulate a pseudonym replacement strategy for mobile nodes. Find the balance strategy of each node by analyzing the n-player scenario of complete or incomplete information. Through this balancing strategy, even in a non-cooperative environment, the best strategy for maintaining privacy can be found.

Boualouache et al. [22] proposed a pseudonym strategy called Silence and Swap at Signalized Intersection (S2SI). This strategy is composed of two protocols. One protocol is responsible for establishing Silent Mix zones (SMs). When the traffic lights are red, vehicles will gather near the traffic signs, so this area is established as SM and managed by RSU. The second is to allow vehicles entering SM to exchange pseudonyms under the management of RSU until the signal light turns green.

In the scheme Ying et al. proposed [23], in order to eliminate the shortcomings of the mix-zone, that is, each mix-zone needs a certain number of vehicles to exchange pseudonyms, so the mix-zone is changed from a fixed mix-zone to a dynamic establishment when the pseudonym of the vehicle is about to expire, the third trusted unit can be requested to assist in establishing the mix-zone. The reputation model is introduced to encourage vehicles to respond to pseudonym exchange requests and to promote cooperation between vehicles in the mix-zone.

In the scheme A. Boualouache et al. proposed in 2016 [24], the mix-zone is served by existing roadside infrastructure such as gas stations. The mix-zone has an entrance called the router and an exit called the aggregator. In the middle of the entrance and exit is an area composed of several lanes. During daily driving, the vehicle will continue to broadcast safety messages until it enters the mix-zone. Vehicles can only leave the mix-zone through the aggregator and must change their pseudonym before leaving. Since the time for each vehicle to receive service in the area is random, such as the time for each vehicle to refuel, the order of entering and leaving the mix-zone is not the same, or the aggregator can directly arrange the order.

4 Proposed Framework

In this section, we describe the scenario and the proposed framework. This framework includes four processes, including system setup, registration phase, region joining phase, and disclosure phase.

4.1 Framework Scenarios

In VANET, many applications such as post-crash notification, cooperative collision warning, and traffic vigilance, require all vehicles cooperate with other vehicles through broadcast Cooperate Awareness Messages (CAMs). If the vehicle cannot authenticate the sender when receiving the message, the vehicle will not be able to distinguish whether the message is trustworthy. In addition, the CAMs broadcast by the vehicle often contain private information about the vehicle. If the privacy of the vehicle is not properly protected, the attacker can perform attacks such as vehicle tracking by analyzing the information.

This paper proposes an anonymous authentication framework for VANET. In this framework, after the vehicle leaves the manufacturer, it will register with the Trust Authority and Registration Authority to obtain the necessary group signature information and the seed used to generate the pseudonym. In addition, we divide a large region into different small regions, and each small region has a regional manager. When the vehicle enters a new region, it must use the self-generated pseudonym and group signature scheme for registration; after registration, the vehicle uses this pseudonym to communicate with other vehicles in the same region. Before the registration is completed, the vehicle cannot communicate with other vehicles. Whenever the vehicle enters a new area or stays in the same area for too long, the vehicle will regenerate the pseudonym and register again with the regional manager.

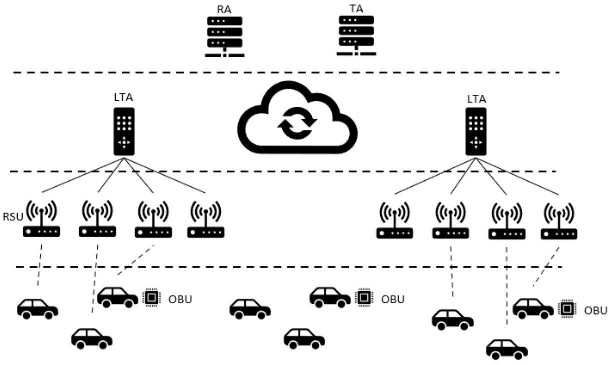


Figure 2. Network architecture of proposed framework

Figure 2 describes the network model of our proposed framework. This framework consists of five different roles: Registration Authority, Trust Authority, Local Trust Authority, Roadside Unit and the last one is Vehicle. We define these roles as follows:

- Registration Authority (RA): It is a Trusted third party in this framework. In our scenario, all vehicles must register with RA and submit vehicle identity after the manufacturers. After the registration is completed, RA will provide a long-term pseudonym to the vehicle, which is called the seed, and it is used to generate the dynamic pseudonym. After registration with the TA, the vehicle submits this seed to the TA for the next step of the registration phase.
- Trust Authority (TA): It is a trusted third party and is also the Group Manager (GM) in the group signature scheme. Mainly have the following responsibilities:
  - Initialization of group signature scheme.
  - TA is responsible for continuing the work of RA. TA will add vehicles to a group in the group signature scheme. And if necessary, the group signature scheme is used to disclose the perpetrator's vehicle.
- Local Trust Authority (LTA): Serving as a regional administrator, each LTA possesses a distinctive identity and oversees a specific region. Upon the

vehicle's entry into the region supervised by the LTA, the vehicle initially employs the seed to create the short-term pseudonym utilized within this area, and then proceeds with the registration using the group signature scheme.

- Roadside Unit (RSU): RSU is the roadside infrastructure in VANET. It has a unique RSUid and is capable of wireless communication with OBU and wired communication with TA, RA, and LTA. The main task is to deliver messages for OBU to communicate with other units or to deliver messages from other infrastructures to OBU. In addition, when the vehicle enters a new region, it will first request the RSU to generate pseudonymous parameters, also called paths. This path is composed of three parameters LTA_{id}, RSU_{id}, and a constant t that all RSUs in the same LTA synchronously change according to time.
- Vehicle: The term "smart vehicle" refers to a vehicle outfitted with an OBU. The OBU facilitates communication with other vehicles (Vehicle to Vehicle communication, i.e., V2V) or communication with other infrastructures (Vehicle to Infrastructure, i.e., V2I). Within the framework proposed in this document, the vehicle offers fundamental computing capabilities, with the OBU broadcasting Cooperative Awareness Messages (CAMs) to neighboring vehicles at a frequency ranging from 1 to 10 Hz. Additionally, the vehicle is equipped with a Trusted Platform Module (TPM) to securely store crucial personal information, such as the group secret key and seed.

4.2 Assumptions

We have the following assumption in the protocol:

1. We assume TA, RA, LTA, and RSU are honest but curious.
2. TA, RA, LTA, and RSU will not collude.
3. TA, as the GM, cannot be compromised by an adversary.
4. TA, RA, and LTA have established a secure channel and use ECDSA to check the identity.
5. Every party keeps its own secret safely.

4.3 Protocol Design

This protocol involves four distinct stages: System Setup, Registration, Region Join, and Disclosure. During the System Setup, we initiate the group signature scheme and create the group manager's secret key, group public key, and group member's secret key. Before any vehicle is operational, it must provide the required information and register with the TA and RA; failure to do so will result in the inability to communicate with others. This process will occur during the Registration Phase. During the Region Join Phase, a vehicle enrolls with the LTA upon entering a new region. The Disclosure Phase will explain our approach to vehicle tracking. In this section, we will elaborate on these four stages within the framework, with all symbols defined in Table 1.

Table 1. The notations and their definitions

Notation	Definition
Vid_i	Real identity of user i
$seed_i$	Seed of user i
gid_i	Group id of user i
$pseudonym_i$	Pseudonym of user i
gid_{LTA}	Group id of LTA
gid_{RSU}	Group id of RSU
$gmsk\ \{a_{TA}, b_{TA}, c_{TA}, d_{TA}\}$	Private key of group manager
n, r, α, β	Public parameter of group signature of same member
p, q, s, h, k	Secret parameters of group signature that group manager keep
$gsk_{i,} gpk_i$	Group private/public key of *i*
$path\ \{LTA_{id}, RSU_{id}, t\}$	Path to generate pseudonym, t is constant
d_i, Q_i	The ECC key pair of user i
M_i	Messages transferred between entities, where i ∊ { 1, 2, …, n }
m_i	Intermediate messages, where i ∊ { 1, 2, …, n }
$\sigma_i\{f_i, g_i\}$	Signature of intermediate message m_i
$S_{i\text{-}j}$	The session key between entity i and j
SK_i, PK_i	ECDSA public key and private key pair.
TS_i	Timestamp
$Enc(k, m)$	Encryption message m with key k
$Dec(k, m)$	Decryption message m with key k
$sign(m, k)$	Sign message m with key k
$Verify(k, m, \sigma)$	Verify signature σ of message m with key k
$hash(m)$	Hash value of message m
$checkTs(TS_i)$	Function to check timestamp TS_i
$checkHonest$	Function to check the honesty of vehicle
$getVid(seed_i)$	Function to get Vid of $seed_i$
$Disclose(m, \sigma)$	Function to disclose the vehicle

4.3.1 System Setup

At this stage, the TA will initially generate a specific number of groups in advance based on demand using the group signature scheme proposed by V.G. Martínez et al. [25]. Every group holds a private key belonging to the group manager, shared by the entire group. Both the group public key and the private key of each group member can generate and verify their own signatures.

1. TA chooses two large prime numbers p and q such that $p = u_1 \cdot r \cdot p_1+1$ and $q = u_2 \cdot r \cdot q_1+1$, where r, q_1, p_1 are prime numbers and u_1, $u_2 \in Z$ with $\gcd(u_1, u_2) = 2$. $u_1 = 2 \cdot v_1$, $u_2 = 2 \cdot v_2$, where v_1, v_2 are prime numbers. To guarantee the security of the scheme, the bit length of r is selected so that the SDLP of order r in Z^*_n is computationally infeasible.
2. TA Computes $n = p \cdot q$, Euler function $\varphi(n) = (p - 1) \cdot (q - 1) = u_1 \cdot u_2 \cdot r^2 \cdot p_1 \cdot q_1$, and Carmichael function $\lambda(n) = \mathrm{lcm}(p - 1, q - 1) = 2 \cdot v_1 \cdot v_2 \cdot r \cdot p_1 \cdot q_1$.
3. TA selects an element $\alpha \in Z^*_n$ with multiplicative order r modulo n, such that $\gcd(\alpha, \varphi(n)) = 1$. The computation of element α is efficient, as TA possesses knowledge of the factorization of n, enabling it to determine φ(n) and subsequently λ(n). In practice, it is enough to find a random value $g \in Z^*_n$ such that $g^{\lambda(n)} \equiv 1(mod\ n)$ and checks that none of the 62 non-trivial divisors of $\lambda(n)$ are the actual order of g. A non-trivial divisor refers to a divisor of λ(n) that is not equal to 1 or λ(n) itself. The count of non-trivial divisors of λ(n) arises from the equation λ(n) = 2 · v1 · v2 · r · p1 · q1, where each factor represents a prime number. After finding the value of g, the generator is acquired by performing the subsequent computation: $\alpha = g^{\lambda(n)/r}\ (mod\ n)$.
4. TA generates a secret number $s \in Z^*_r$ and determines $\beta = \alpha^s\ (mod\ n)$.
5. TA will publish values n, r, α and β, and keep p, q, s secretly.
6. TA sets its private key by generating four random numbers a_{TA}, b_{TA}, c_{TA}, $d_{TA} \in Z^*_n$
7. TA determines the shared public key for G by computing

$$P = \alpha^{a_{TA}} \beta^{b_{TA}} (mod\ \ n) = \alpha^{a_{TA}+s \cdot b_{TA}} (mod\ \ n)\,. \qquad (1)$$

$$L = \alpha^{c_{TA}} \beta^{d_{TA}} (mod\ \ n) = \alpha^{c_{TA}+s \cdot d_{TA}} (mod\ \ n)\,. \qquad (2)$$

8. TA computes the integers h, $k \in Z_r$ such that $h = a_{TA} + s \cdot b_{TA}\ (\mathrm{mod}\ r)$ and $k = c_{TA} + s \cdot d_{TA}\ (\mathrm{mod}\ r)$
9. TA determines the private key for each signer $U_i \in G$, $1 \le i \le t$, where each private key is the tuple $\{a_i, b_i, c_i, d_i\}$ and a_i, b_i, c_i, $d_i \in Z_r$. To do that, TA first generates x pairs of random numbers, b_i, $d_i \in Z_r$. After that, it obtains the remaining elements by using the following equations:

$$a_i = h - s \cdot b_i \left(mod\, r\right). \qquad (3)$$

$$c_i = k - s \cdot d_i \left(mod\, r\right). \qquad (4)$$

4.3.2 Registration Phase

Each vehicle engaged in this framework must undergo registration. Initially, the OBU submits the Vid_i to the RA. Subsequently, upon Vid_i reception, the RA selects necessary terms from the wordlist to form a mnemonic, using the PBKDF2 key derivation function to generate $seed_i$. The $seed_i$ serves as the long-term pseudonym within this framework, with the $\{seed_i, Vid_i\}$ combination stored in the RA's database.

Once the RA transfers the seed to the TA, the TA incorporates the seed into the pre-established group during the system setup phase. The TA retains the subsequent tuples $\{seed_i, gid_i, gpk_i, n, r, \alpha, \beta, s, h, k, a_i, b_i\}$, while $seed_i, gid_i$, gpk_i, gsk_i, n, r, α, β and gpk_{LTA} are transmitted to the OBU following the completion of registration. Upon reception of the group signature information, the OBU can utilize the following equations to authenticate the signature of $gsk_i\{a_i, b_i, c_i, d_i\}$ signed by $gpk_i\{P_i, L_i\}$:

$$P_i = \alpha^{a_i} \beta^{b_i} \ \left(mod\, n\right). \qquad (5)$$

$$L_i = \alpha^{c_i} \beta^{d_i} \ \left(mod\, n\right). \qquad (6)$$

4.3.3 Region Joining Phase

Upon entering different regions, each vehicle must request the LTA of the area to join. The OBU requests the first RSU encountered upon entering the area to acquire the present pseudonymous generation parameter, $path$ $\{LTA_{id}, RSU_{id}, t\}$. The RSU initially generates $M_5 = \{m_5, \sigma_5\}$, where $m_5 = \{path, TS_1\}$, and σ_5 represents the output, with the RSU signing the hash value of m_5 using its own group secret key gsk_{RSU}, while TS_1 denotes the timestamp, as shown in Figure 3.

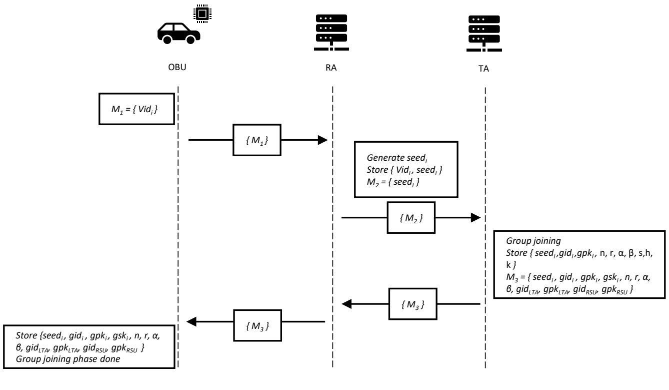
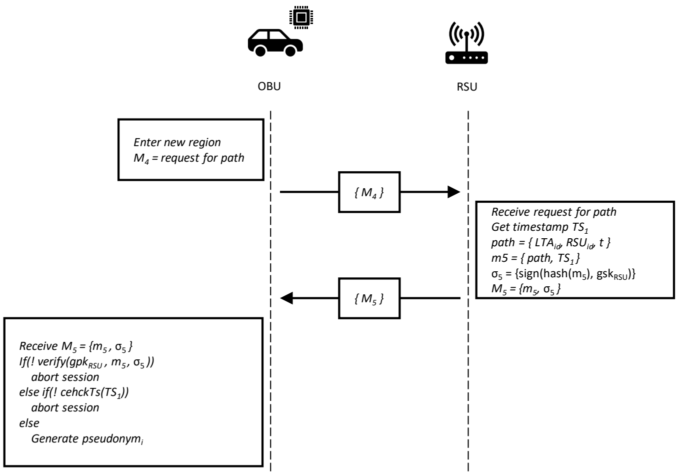

OBU
RA
TA
M1 = { Vidi }
{ M1 }
Generate seedi
Store { Vidi, seedi }
M2 = { seedi }
{ M2 }
Group joining
Store { seedi,gidi,gpki, n, r, α, β, s,h, k }
M3 = { seedi, gidi, gpki, gski, n, r, α, β, gidLTA, gpkLTA, gidRSU, gpkRSU }
{ M3 }
{ M3 }
Store {seedi, gidi, gpki, gski, n, r, α, β, gidLTA, gpkLTA, gidRSU, gpkRSU }
Group joining phase done

Figure 3. Registration phase authentication flow

After obtaining M_5, the OBU verifies σ_5 using the function $verify(gpk_{RSU}, m_5, \sigma_5)$ and checks TS_1 using the function $checkTs(TS_1)$. Upon successful verification, the OBU proceeds to generate the pseudonym. The path acquired by the OBU consists of a total of three parameters, implying that the pseudonym derivation will be performed thrice to obtain the pseudonym used within the area, as shown in Figure 4.



```
Enter new region
$M_4$ = request for path
```

```
Receive request for path
Get timestamp $TS_1$
path = { $LTA_{id}$, $RSU_{id}$, t }
m5 = { path, $TS_1$ }
$\sigma_5$ = {sign(hash($m_5$), $gsk_{RSU}$)}
$M_5$ = {$m_5$, $\sigma_5$ }
```

```
Receive $M_5$ = {$m_5$ , $\sigma_5$ }
If(! verify($gpk_{RSU}$ , $m_5$, $\sigma_5$ ))
   abort session
else if(! cehckTs($TS_1$))
   abort session
else
   Generate $pseudonym_i$
```

Figure 4. Region joining phase path request flow

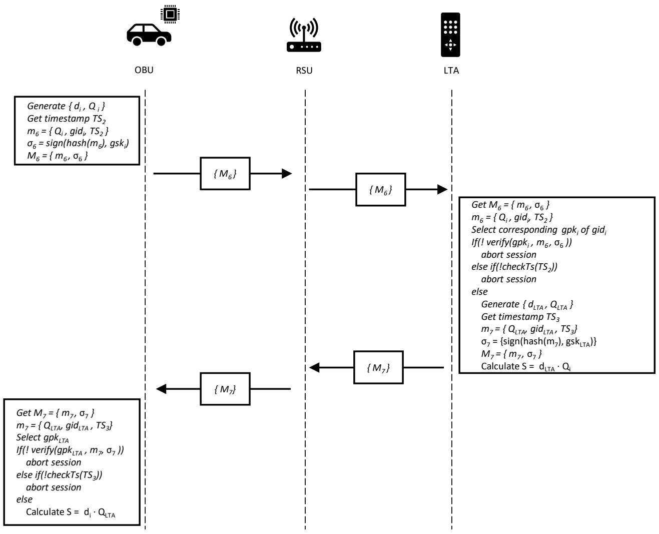
Here, we make reference to the method of generating sub-keys within the HD wallet. Initially, we conduct HMAC-SHA512 on the seed, resulting in a 512-bit value. This value is then split into two halves of 256 bits each. The left half corresponds to the master private key, while the right half corresponds to the master chain code. When generating subsequent layers of the key, three parameters are required:

- Parent public key: After deriving the master private key, the next step involves calculating the corresponding public key based on ECC using the master private key.
- Parent chain code: To enhance the security of the subkey derivation process and prevent deducing the subkey solely from the parent private key, an additional 256 bits, termed the chain code, are introduced. This chain code is derived from the right half of the 256-bit value obtained from the HMAC-SHA512 operation.
- Index: This is a 2^{32}-bit number. During the HMAC-SHA512 operation, this index is concatenated after the parent public key. This indexing mechanism allows each layer's key to generate 2^{32} subkeys.

Upon acquiring the necessary parameters and generating the pseudonym, the vehicle initiates the registration process. To ensure the security of communication, the OBU and LTA perform the ECDHE process to establish a secure channel, as shown in Figure 5. Initially, the vehicle generates a private and public ECC key pair, represented by d_i and Q_i, and commences the ECDHE negotiation with LTA. As shown in Figure 4, the OBU generates an intermediate message, $m_6 = \{Q_i, gid_i, TS_2\}$. Subsequently, the OBU signs the message m$_6$ using gsk_i, utilizing the following two formulas to obtain the signature $\sigma_6\{f_6, g_6\} = sign(hash(m_6), gsk_i)$. The OBU then transmits the message $M_6 = \{m_6, \sigma_6\}$ to LTA.

$$f_i = a_i + c_i m_i \left(mod\, r\right). \tag{7}$$

$$g_i = b_i + d_i m_i \left(mod\, r\right). \tag{8}$$



```
Generate { $d_i$ , $Q_i$ }
Get timestamp $TS_2$
$m_6$ = { $Q_i$ , $gid_i$, $TS_2$ }
$\sigma_6$ = sign(hash($m_6$), $gsk_i$)
$M_6$ = { $m_6$, $\sigma_6$ }
```

```
Get $M_6$ = { $m_6$, $\sigma_6$ }
$m_6$ = { $Q_i$ , $gid_i$, $TS_2$ }
Select corresponding $gpk_i$ of $gid_i$
If(! verify($gpk_i$ , $m_6$, $\sigma_6$ ))
   abort session
else if(!checkTs($TS_2$))
   abort session
else
   Generate { $d_{LTA}$ , $Q_{LTA}$ }
   Get timestamp $TS_3$
   $m_7$ = { $Q_{LTA}$, $gid_{LTA}$ , $TS_3$}
   $\sigma_7$ = {sign(hash($m_7$), $gsk_{LTA}$)}
   $M_7$ = { $m_7$, $\sigma_7$ }
   Calculate S = $d_{LTA} \cdot Q_i$
```

```
Get $M_7$ = { $m_7$, $\sigma_7$ }
$m_7$ = { $Q_{LTA}$, $gid_{LTA}$ , $TS_3$}
Select $gpk_{LTA}$
If(! verify($gpk_{LTA}$ , $m_7$, $\sigma_7$ ))
   abort session
else if(!checkTs($TS_3$))
   abort session
else
   Calculate S = $d_i \cdot Q_{LTA}$
```

Figure 5. Region Joining Phase secure channel establish flow

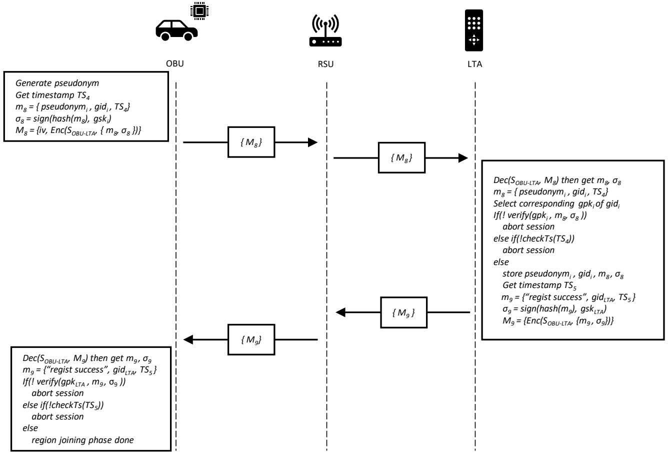
After LTA received message M_6 from OBU, LTA will check the data integrity by $verify(gpk_i, m_6, \sigma_6)$ through formula 7 and $checkTs(TS_2)$:

$$P_i L_i^{m_i} = \alpha^{f_i} \beta^{g_i} \left(mod\, n\right). \tag{9}$$

Upon verifying the group signature, the Local Trust Authority (LTA) generates an ECC private and public key pair, represented as d_{LTA} and Q_{LT}, respectively. Subsequently, LTA generates an intermediate message, $m_7 = \{Q_{LTA}, gid_{LTA}, TS_3\}$, and its corresponding group signature, $\sigma_7 = sign(hash(m_7), gsk_{LTA})$. Upon generating m_7 and σ_7, LTA transmits $M_7 = \{m_7, \sigma_7\}$ to the OBU. Upon receiving M_7, the OBU verifies the data integrity using $verify(gpk_{LTA}, m_7, \sigma_7)$ through formula 7, and cross-checks with $checkTs(TS_3)$. Once the OBU obtains the public key of LTA and LTA acquires the public key of OBU, both entities can compute a shared secret, $S_{OBU\text{-}LTA} = d_i \cdot Q_{LTA} = d_{LTA} \cdot Q_i$.

Once the secure channel is established, the OBU initiates the transmission of essential registration information to the LTA, including the short-term pseudonym designated for the particular area. The OBU creates an intermediate message $m_8 = \{pseudonym_i, gid_i, TS_4\}$ and the signature σ_8. The OBU encrypts m_8 and σ_8 to form $M_8 = Enc(S_{OBU\text{-}LTA}, (m_8, \sigma_8))$, which is then transferred to the LTA. Upon receiving M_8, the LTA decrypts it to obtain m_8, verifies the signature, and validates the timestamp. Assuming the verification process succeeds, the LTA sends a success confirmation message back to the OBU. In response, the LTA generates an intermediate message, denoted as $m_9 = \{$"registration success," $gid_{LTA}, TS_5\}$, which is signed using the group secret key gsk_{LTA} to yield $\sigma_9 = sign(hash(m_9), gsk_{LTA})$. Finally, the LTA encrypts the content as $M_9 = Enc(S_{OBU\text{-}LTA}, (m_9, \sigma_9))$, and forwards it to the OBU.

Following the receipt of M_9, the OBU verifies m_9. In the event of a successful validation, the OBU can communicate with other vehicles within the same region as $pseudonym_i$. However, if the verification process fails, the region joining phase is immediately terminated, as shown in Figure 6.



```
Generate pseudonym
Get timestamp $TS_4$
$m_8$ = { $pseudonym_i$ , $gid_i$ , $TS_4$ }
$\sigma_8$ = sign(hash($m_8$), $gsk_i$)
$M_8$ = {iv, Enc($S_{OBU\text{-}LTA}$, { $m_8$, $\sigma_8$ })}
```

```
Dec($S_{OBU\text{-}LTA}$, $M_8$) then get $m_8$, $\sigma_8$
$m_8$ = { $pseudonym_i$ , $gid_i$ , $TS_4$ }
Select corresponding $gpk_i$ of $gid_i$
If(! verify($gpk_i$ , $m_8$, $\sigma_8$ ))
   abort session
else if(!checkTs($TS_4$))
   abort session
else
   store $pseudonym_i$ , $gid_i$ , $m_8$, $\sigma_8$
   Get timestamp $TS_5$
   $m_9$ = {"regist success", $gid_{LTA}$, $TS_5$ }
   $\sigma_9$ = sign(hash($m_9$), $gsk_{LTA}$)
   $M_9$ = {Enc($S_{OBU\text{-}LTA}$, { $m_9$, $\sigma_9$ })}
```

```
Dec($S_{OBU\text{-}LTA}$, $M_9$) then get $m_9$, $\sigma_9$
$m_9$ = {"regist success", $gid_{LTA}$, $TS_5$ }
If(! verify($gpk_{LTA}$ , $m_9$, $\sigma_9$ ))
   abort session
else if(!checkTs($TS_5$))
   abort session
else
   region joining phase done
```

Figure 6. Region Joining Phase registration flow

4.3.4 Vehicle Disclosure Phase

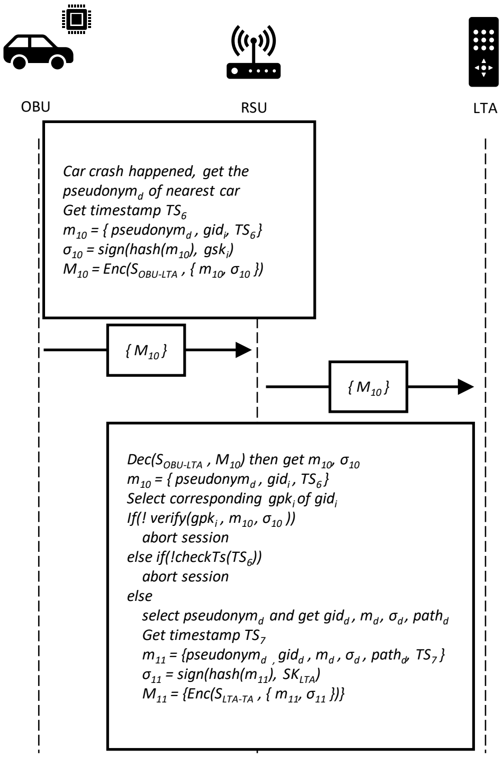
In the event of a car accident, due to the continuous broadcasting of its location at regular intervals, the involved vehicle can determine the nearest neighboring vehicle at the time of the collision. Subsequently, during the disclosure phase, the vehicle establishes a secure communication channel with the LTA after completing the region joining phase with the LTA. The initial action entails providing the LTA with the $pseudonym_d$, of the nearest vehicle recorded during the occurrence of the accident.

At the time of the accident, the affected vehicle identifies the pseudonym that requires disclosure, designated as $pseudonym_d$, alongside its own group ID, gidi, and TS_6, to produce generate $m_{10} = \{pseudonym_d, gid_i, TS_6\}$ and the signature σ_{10}. After that, the OBU creates message M_{10}=$Enc(S_{OBU\text{-}LTA}, (m_{10}, \sigma_{10}))$ and transmits it to the LTA, as shown in Figure 7.

Upon receiving the disclosure request message from the OBU, the LTA decrypts M_{10} to obtain m_{10} and σ_{10}. If the verification is successful, LTA searches the corresponding registration record of $pseudonym_d$, which is the information that LTA received of the region joining phase, including the registration message m_d, group signature $\sigma_d\{f_d, g_d\}$ of m_d, gid_d, the $path_d\{LTA_{id}, RSU_{id}, t\}$ of $pseudonym_d$. Subsequently, the LTA generates m_{11} where TS_7 is a timestamp. It further creates a signature σ_{11}, and transmits $M_{11} = Enc(S_{LTA\text{-}TA}, (m_{11}, \sigma_{11}))$ to the TA to disclose the signer of signature afterward.

Upon receiving and decrypting message M_{11}, the TA obtains m_{11} and the signature σ_{11}. Subsequently, TA verifies the data integrity through $verify(gpk_i, m_6, \sigma_6)$ and checks the validity of TS_7. If the verification is successful, TA proceeds with the vehicle disclosure phase. It executes the disclose function, $disclose(m_d, \sigma_d)$ to iterate all the registration records of gid_d, aiming to identify the $seed_d$ of the signer associated with σ_d.

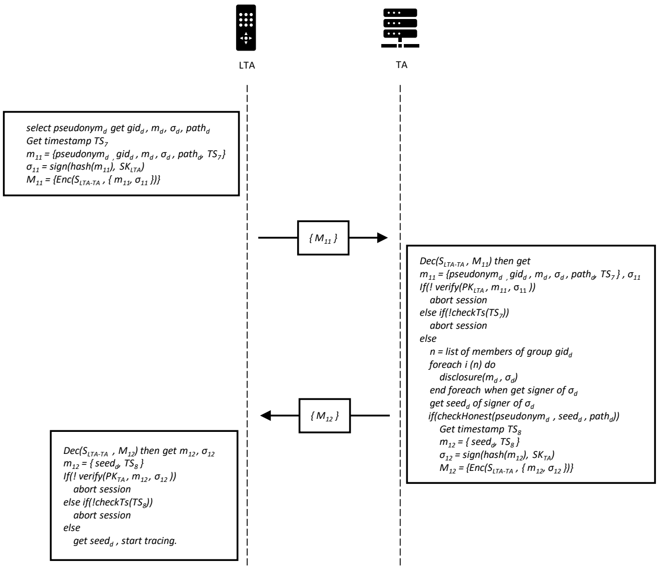
$$\left.\begin{aligned}\bar{f}_d &= a_i + c_i m_d \left(mod\, r\right)\\ \bar{g}_d &= b_i + d_i m_d \left(mod\, r\right)\end{aligned}\right\}, \text{where } 1 \le i \le x. \tag{10}$$



```
Car crash happened, get the
$pseudonym_d$ of nearest car
Get timestamp $TS_6$
$m_{10}$ = { $pseudonym_d$ , $gid_i$, $TS_6$ }
$\sigma_{10}$ = sign(hash($m_{10}$), $gsk_i$)
$M_{10}$ = Enc($S_{OBU\text{-}LTA}$ , { $m_{10}$, $\sigma_{10}$ })
```

```
Dec($S_{OBU\text{-}LTA}$ , $M_{10}$) then get $m_{10}$, $\sigma_{10}$
$m_{10}$ = { $pseudonym_d$ , $gid_i$ , $TS_6$ }
Select corresponding $gpk_i$ of $gid_i$
If(! verify($gpk_i$ , $m_{10}$, $\sigma_{10}$ ))
   abort session
else if(!checkTs($TS_6$))
   abort session
else
   select $pseudonym_d$ and get $gid_d$ , $m_d$ , $\sigma_d$ , $path_d$
   Get timestamp $TS_7$
   $m_{11}$ = { $pseudonym_d$ , $gid_d$ , $m_d$ , $\sigma_d$ , $path_d$, $TS_7$ }
   $\sigma_{11}$ = sign(hash($m_{11}$), $SK_{LTA}$)
   $M_{11}$ = {Enc($S_{LTA\text{-}TA}$ , { $m_{11}$, $\sigma_{11}$ })}
```

Figure 7. Vehicle informs LTA of the pseudonym



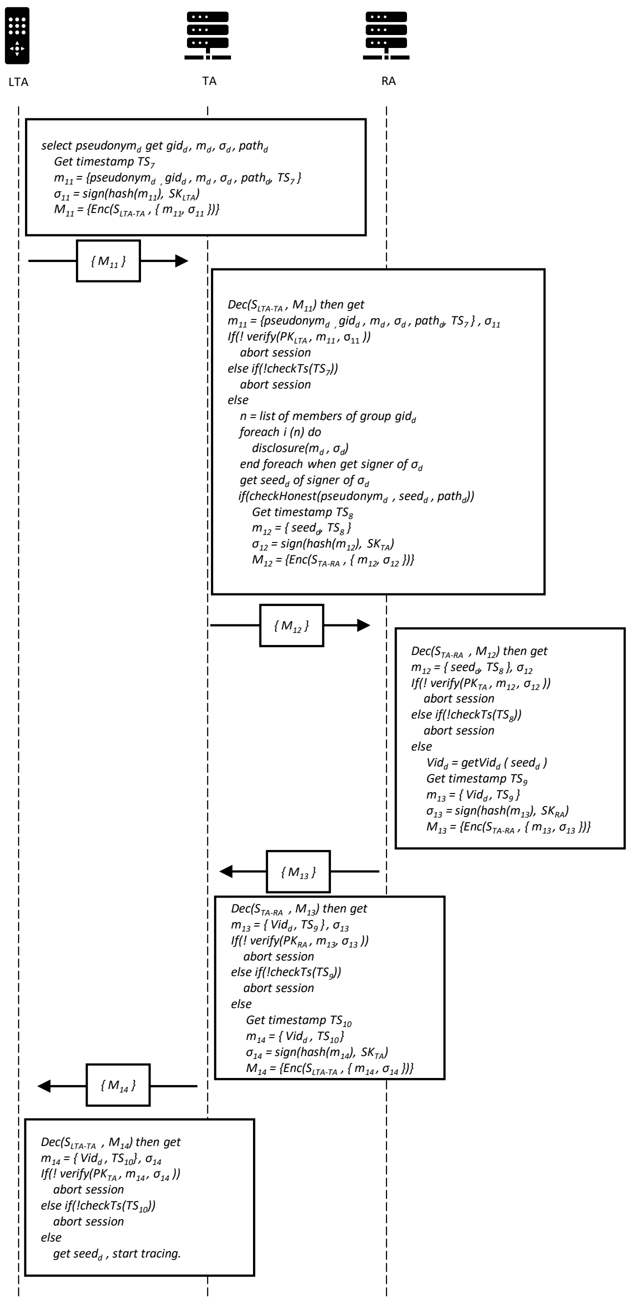
```
select $pseudonym_d$ get $gid_d$ , $m_d$, $\sigma_d$, $path_d$
Get timestamp $TS_7$
$m_{11}$ = { $pseudonym_d$ , $gid_d$ , $m_d$ , $\sigma_d$ , $path_d$, $TS_7$ }
$\sigma_{11}$ = sign(hash($m_{11}$), $SK_{LTA}$)
$M_{11}$ = {Enc($S_{LTA\text{-}TA}$ , { $m_{11}$, $\sigma_{11}$ })}
```

```
Dec($S_{LTA\text{-}TA}$ , $M_{11}$) then get
$m_{11}$ = { $pseudonym_d$ , $gid_d$ , $m_d$ , $\sigma_d$ , $path_d$, $TS_7$ } , $\sigma_{11}$
If(! verify($PK_{LTA}$ , $m_{11}$ , $\sigma_{11}$ ))
   abort session
else if(!checkTs($TS_7$))
   abort session
else
   n = list of members of group $gid_d$
   foreach i (n) do
      disclosure($m_d$ , $\sigma_d$)
   end foreach when get signer of $\sigma_d$
   get $seed_d$ of signer of $\sigma_d$
   if(checkHonest($pseudonym_d$ , $seed_d$ , $path_d$))
      Get timestamp $TS_8$
      $m_{12}$ = { $seed_d$, $TS_8$ }
      $\sigma_{12}$ = sign(hash($m_{12}$), $SK_{TA}$)
      $M_{12}$ = {Enc($S_{LTA\text{-}TA}$ , { $m_{12}$, $\sigma_{12}$ })}
```

```
Dec($S_{LTA\text{-}TA}$ , $M_{12}$) then get $m_{12}$, $\sigma_{12}$
$m_{12}$ = { $seed_d$, $TS_8$ }
If(! verify($PK_{TA}$ , $m_{12}$, $\sigma_{12}$ ))
   abort session
else if(!checkTs($TS_8$))
   abort session
else
   get $seed_d$ , start tracing.
```

Figure 8. The process if a disclosed vehicle is honest

Upon identifying the corresponding $seed_d$, TA verifies the correctness of generating the short-term pseudonym once again, as shown in Figure 8. This verification is carried out based on the $checkHonest$ function to confirm the integrity of the $path_d$ and $seed_d$. If checked, TA will generate intermediate message $m_{12} = \{seed_d, TS_8\}$ and sign m_{12} to get $\sigma_{12} = sign(hash(m_{12}), SK_{TA})$ then transmit $M_{12} = Enc(S_{LTA\text{-}TA}, (m_{12}, \sigma_{12}))$ to inform LTA to assistance in tracing the location of $seed_d$. While receiving M_{12}, LTA decrypt message M_{12} by executing $Dec(S_{LTA\text{-}TA}, M_{12})$ to get $m_{12} = \{seed_d, TS_8\}$ and $\sigma_{12} = sign(hash(m_{12}), SK_{TA})$. Furthermore, LTA verifies m_{12} by executing $verify(PK_{TA}, m_{12}, \sigma_{12})$ and checks (TS_8); if σ_{12} and TS_8 are verified, LTA is stores seed and will try to trace the vehicle, as shown in Figure 9.



```
select $pseudonym_d$ get $gid_d$, $m_d$, $\sigma_d$, $path_d$
    Get timestamp $TS_7$
    $m_{11} = \{pseudonym_d, gid_d, m_d, \sigma_d, path_d, TS_7\}$
    $\sigma_{11} = sign(hash(m_{11}), SK_{LTA})$
    $M_{11} = \{Enc(S_{LTA\text{-}TA}, \{m_{11}, \sigma_{11}\})\}$
```

```
$Dec(S_{LTA\text{-}TA}, M_{11})$ then get
$m_{11} = \{pseudonym_d, gid_d, m_d, \sigma_d, path_d, TS_7\}, \sigma_{11}$
If(! verify($PK_{LTA}$, $m_{11}$, $\sigma_{11}$ ))
    abort session
else if(!checkTs($TS_7$))
    abort session
else
    n = list of members of group $gid_d$
    foreach i (n) do
        disclosure($m_d$, $\sigma_d$)
    end foreach when get signer of $\sigma_d$
    get $seed_d$ of signer of $\sigma_d$
    if(checkHonest($pseudonym_d$, $seed_d$, $path_d$))
        Get timestamp $TS_8$
        $m_{12} = \{seed_d, TS_8\}$
        $\sigma_{12} = sign(hash(m_{12}), SK_{TA})$
        $M_{12} = \{Enc(S_{TA\text{-}RA}, \{m_{12}, \sigma_{12}\})\}$
```

```
$Dec(S_{TA\text{-}RA}, M_{12})$ then get
$m_{12} = \{seed_d, TS_8\}, \sigma_{12}$
If(! verify($PK_{TA}$, $m_{12}$, $\sigma_{12}$ ))
    abort session
else if(!checkTs($TS_8$))
    abort session
else
    $Vid_d = getVid_d(seed_d)$
    Get timestamp $TS_9$
    $m_{13} = \{Vid_d, TS_9\}$
    $\sigma_{13} = sign(hash(m_{13}), SK_{RA})$
    $M_{13} = \{Enc(S_{TA\text{-}RA}, \{m_{13}, \sigma_{13}\})\}$
```

```
$Dec(S_{TA\text{-}RA}, M_{13})$ then get
$m_{13} = \{Vid_d, TS_9\}, \sigma_{13}$
If(! verify($PK_{RA}$, $m_{13}$, $\sigma_{13}$ ))
    abort session
else if(!checkTs($TS_9$))
    abort session
else
    Get timestamp $TS_{10}$
    $m_{14} = \{Vid_d, TS_{10}\}$
    $\sigma_{14} = sign(hash(m_{14}), SK_{TA})$
    $M_{14} = \{Enc(S_{LTA\text{-}TA}, \{m_{14}, \sigma_{14}\})\}$
```

```
$Dec(S_{LTA\text{-}TA}, M_{14})$ then get
$m_{14} = \{Vid_d, TS_{10}\}, \sigma_{14}$
If(! verify($PK_{TA}$, $m_{14}$, $\sigma_{14}$ ))
    abort session
else if(!checkTs($TS_{10}$))
    abort session
else
    get $seed_d$, start tracing.
```

Figure 9. The process if the disclosed vehicle is dishonest

If checkHonest fails, TA requests RA to reveal the Vid_d associated with $seed_d$. TA generates an intermediate message m_{12}, and the signature σ_{12}, and transmits $M_{12} = Enc(S_{LTA\text{-}TA}, (m_{12}, \sigma_{12}))$ to inform RA to disclose the actual identity of the vehicle. Upon receiving M_{12}, RA decrypts it, verifies data integrity, and checks the validity of TS_8. If successful, RA uses $seed_d$ to retrieves Vid_d, and passes M_{13} to TA. With this process complete, law enforcement can trace the vehicle through its real identity.

5 Experiment and Analysis

This section is divided into two sections. The initial part focuses on delineating the experimental environment and presenting the results. Subsequently, the second part conducts a comprehensive analysis to assess the security robustness of the protocol proposed in this paper.

5.1 Experiment Environment and Result

In this section, we'll perform experiments related to the region joining phase to assess the performance during the vehicle's entry into a new area. This includes testing the process from requesting parameters with RSU to establishing a secure channel and completing registration. The initial part of the experiment involves setting up the three roles of the region join phase (OBU, RSU, and LCA) on two separate hosts, with the specifications of these computers detailed in Table 2:

Table 2. Experiment environment

Component Computer	CPU	RAM
Computer 1	Intel i5-4210M	8GB
Computer 2	Intel i7-8700K	16GB

In the absence of an actual vehicle for experimentation, we simulate the OBU on the first computer using a Maven project programmed in Java OpenJDK 14 on Windows 10. Three different scenarios are simulated based on the peak traffic flow data from the Ministry of Transport of Taiwan [26]. In scenario 1, 100 vehicles enter the region and request to join per minute, representing the least traffic among the three scenarios. In scenario 2, 200 vehicles enter the region per minute; in scenario 3, 300 vehicles enter per minute.

The second host simulates the roles of RSU and LTA. The LTA uses Sqlite3 as its database. The network speeds of both computers are tested using the Dr. Speed tool provided by Chungwa Telecom [27]. The first host has a download speed of 114.96 Mbps and an upload speed of 28.60 Mbps, while the second host has a download speed of 920.74 Mbps and an upload speed of 709.57 Mbps.

Figure 10 illustrates the average time across all stages in three experiment scenarios. Scenario 1 exhibits the best average performance time at 171.68ms. Scenario 2 is approximately 20% slower than Scenario 1, with an average process time of 206.63ms. Scenario 3 demonstrates the poorest performance, being 9% slower than Scenario 2, with an average process time of 225.5ms.

Analyzing the four stages depicted in Figure 10, aside from pseudonym generation, the remaining three stages show a noticeable increase. Among these, the registration with LTA experiences the most significant increase. While there is a slight time increase between Scenario 2 and Scenario 1 in the stage of establishing a secure channel, the impact is not substantial between Scenario 2 and Scenario 3. This suggests that the most pronounced impact on the Region Joining Phase lies in the final registration phase with LTA.

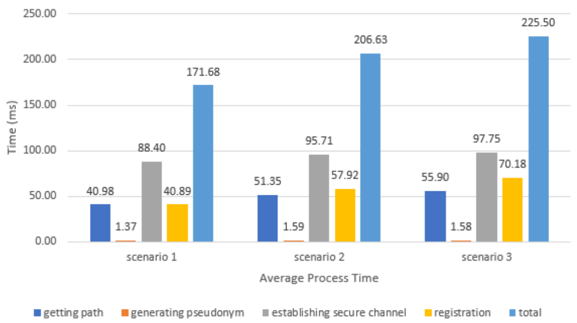


Figure 10. Average process time across various phases in different scenarios

5.2 Experiment Environment and Result

In this section, we perform an in-depth analysis to evaluate the security robustness of the suggested protocol. Our thorough examination will explore diverse facets of the protocol's design, implementation, and potential vulnerabilities.

● **Defense against man-in-the-middle Attack**

In a man-in-the-middle attack against our framework, the attacker will monitor the key agreement message of the Region Joining Phase and try to act as an intermediate party between the LTA and the vehicle. They will then manipulate the message, such as changing the pseudonym that enters the region.

In the proposed framework, the vehicle has already been registered with the TA to obtain the group member's secret key before driving. This process enables the LTA to confirm the vehicle's registration with both the TA and RA when the vehicle is required to join a new region. Additionally, even if the attacker obtains the exchanged public key during key aggregation, based on the computational difficulty of ECC, the attacker cannot reverse-calculate the private key of the vehicle to determine the shared secret between the vehicle and LTA. Thus, the framework we proposed can defend against man-in-the-middle attacks.

● **Defense against Replay Attack**

In the context of a replay attack on this framework, the attacker will observe the key agreement message during the Regions Joining Phase between the LTA and the vehicle. They will store the message transmitted from the vehicle to the LTA and subsequently disguise it as a legitimate attempt by a vehicle to join the region.

In the proposed framework, whenever two entities transmit a message, they are required to append a timestamp to the message, concatenate it, and employ either the group signature mechanism or ECDSA to sign the complete message. Upon receiving the message, the recipient verifies the integrity of the data and then checks whether the timestamp meets the specified criteria. Consequently, the framework proposed in this thesis is designed to thwart replay attacks.

● **Defense against Brute Force Attack**

In a brute force attack against this framework, the attacker will attempt to obtain the seed of a random pseudonym. Once the attacker discovers this seed, he or she will then use it to impersonate the victim.

A mnemonic sentence consists of 12 characters, and the wordlist comprises 2048 words. The probability of any mnemonic sentence is calculated as 2048!/(2048-12)!=5.271538x10^{39}. Assuming the attacker has acquired the path of a generated pseudonym, one million mnemonics can be generated per second. A total of 3.1536x10^{13} pseudonyms can be generated in one year. If the attacker intends to traverse all the pseudonyms of the path, it will require approximately 1.6715937 x 10^{26} years to complete the traversal. Thus, the framework proposed in this thesis is effective in defending against brute force attacks.

● **Identity Anonymity Based on Group Signature**

In the proposed framework, every vehicle is required to register with TA and RA to acquire the parameters associated with the seed for generating short-term pseudonyms and the group member's private key for the group signature scheme used in message signing. Upon entering a distinct area managed by LTA, the vehicle will generate a unique pseudonym specific to that area using the seed and necessary parameters. Consequently, in different areas, each vehicle will utilize distinct pseudonyms for communication. Additionally, leveraging the group signature mechanism, LTA only needs to verify whether the vehicle has registered with TA and RA, without needing knowledge of the vehicle's identity, thereby ensuring the anonymity of the vehicle.

● **Vehicle Unlinkability**

The pseudonym utilized by each vehicle upon entering a new region serves as the vehicle's identity in that area for the subsequent period within the same region. In our framework, all pseudonyms are generated from a seed, involving three iterations of HMAC-SHA 512 and one ECC process. Within our framework, each region possesses a 232-bit constant value synchronized with the LTA and RSU, referred to as the index, which changes over time. This index and unique LTA and RSU identities are employed in the pseudonym derivation process. Leveraging the characteristics of the hash function, any alterations to the input lead to corresponding changes in the output value. Consequently, when individuals are legally driving the vehicle, whether it remains in the same region or not, any two pseudonyms of the vehicle are unlinkable, ensuring the privacy of the vehicle's identity.

● **Accountability**

The group manager, also known as TA, distributes the group member's secret key to each member of the group. Because the group member secret key of any member within the same group can be authenticated using the common group public key, entities like LTA can only ascertain the validity of the signature without discerning the specific identity. Collaboration between LTA and TA, however, provides them with the capability to identify the signer. Consequently, if the signer utilizes their own secret key for signing, they cannot impersonate or deceive other members.

In our framework, vehicles adopt a short-term pseudonym, which is generated from a seed, as their transient identity for communication with other vehicles while in motion. All vehicles can ability to update the seed by re-registering with TA and RA. Since all pseudonyms of a particular vehicle stem from the same seed, tracking the vehicle across regions becomes possible if the seed, path of the pseudonym, and the pseudonym itself are known, and the vehicle successfully passes the honesty check. This crossregional tracking can be accomplished without revealing the V_{id} (vehicle identification) of the vehicle. However, if the vehicle fails the honesty check, we will resort to directly using the V_{id} for tracking. Table 3 illustrates the comparison with other research.

Table 3. Comparison with others

	Ours	[13]	[15]	[20]
Method	Group signature	PKI oriented	ID-based	Symmetric crypto
Network model	De-centralized	Centralized	De-centralized	Centralized
Accountability	Yes	Yes	Yes	No
Vehicle unlinkability	Yes	No	Yes	Yes
Traceability	Yes	No	Yes	No

6 Conclusion

This paper introduces a multi-layered vehicular ad-hoc network architecture designed to ensure the conditional anonymity and traceability of vehicles.

In the proposed method, a vehicle can generate a pseudonym and obtain a personal secret key for the group signature mechanism, enabling the signing of messages with privacy while preserving accountability. When there arises a necessity to disclose a vehicle, the system can assess the honesty of the vehicle to decide whether to reveal its actual identity.

In the experimental results, the average time for vehicles to complete registration with LTA is less than 300 milliseconds. Additionally, the security analysis demonstrates that our protocol is effective in defending against contemporary cyber-attacks, including replay attacks, man-in-the-middle attacks, and brute force attacks.

Acknowledgements

This work is supported by the National Science and Technology Council, Taiwan, under Grant. NSTC 112-2221-E-011-092-MY2 and the National Defense Science and Technology Academic Collaborative Research Project, Taiwan.

References

[1] C. Englund, L. Chen, A. Vinel, S. Y. Lin, Future applications of VANETs, in: C. Campolo, A. Molinaro, R. Scopigno (Eds.), *Vehicular Ad-hoc Networks*, Springer, Cham, 2015, pp. 525–544.

[2] National Police Agency, Ministry of the Interior, *Yearly Statistics of Police Administration*, https://www.npa.gov.tw/static/ebook/Y110/mobile/ index.html, 2022.

[3] C.-C. Hsu, H.-P. Wang, An Analysis of Major Issues Concerning Hit-and-run Accidents Investigation, *Journal of Traffic Science*, Vol. 17, No. 1, pp. 39–56, May, 2017.

[4] European Commission, *2018 Reform of EU Data Protection Rules*, https://ec.europa.eu/commission/ sites/beta-political/files/data-protection-factsheet- changes_en.pdf, 2018.

[5] M. Gerlach, Assessing and Improving Privacy in VANETs, *ESCAR, Embedded Security in Cars*, 2006, pp. 1–9.

[6] B. Wiedersheim, Z. Ma, F. Kargl, P. Papadimitratos, Privacy in Inter-vehicular Networks: Why Simple Pseudonym Change is not Enough, *2010 Seventh International Conference on Wireless on-demand Network Systems and Services (WONS)*, Kranjska Gora, Slovenija, 2010, pp. 176–183.

[7] P. Wuille, *BIP32: Hierarchical Deterministic wallets*, https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, 2012.

[8] M. Palatinus, P. Rusnak, A. Voisine, S. Bowe, *BIP39: Mnemonic Code for Generating Deterministic Keys*, https:// github.com/ bitcoin/ bips/blob/master/bip-0039.mediawiki, 2013.

[9] M. Palatinus, P. Rusnak, *BIP 44: Multi-Account Hierarchy for Deterministic Wallets*, https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki, 2014.

[10] D. Chaum, E. Van Heyst, Group Signatures, *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques*, Brighton, UK, 1991, pp. 257–265.

[11] S. Nakamoto, *A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, pp. 1–9, 2008.

[12] D. Eckhoff, C. Sommer, T. Gansen, R. German, F. Dressler, Strong and Affordable Location Privacy in VANETs: Identity Diffusion using Time-slots and Swapping, *2010 IEEE Vehicular Networking Conference*, New Jersey, NJ, USA, 2010, pp. 174–181.

[13] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, D. C. Parkes, Non-cooperative Location Privacy, *IEEE Transactions on Dependable and Secure Computing*, Vol. 10, No. 2, pp. 84–98, March-April, 2013.

[14] H. Lu, J. Li, M. Guizani, A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs, *2012 Computing, Communications and Applications Conference*, Hong Kong, China, 2012, pp. 345–350.

[15] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response, *IEEE Transactions on Computers*, Vol. 65, No. 8, pp. 2562–2574, August, 2016.

[16] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed Aggregate Privacy-preserving Authentication in VANETs, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 18, No. 3, pp. 516–526, March, 2017.

[17] H. Liu, H. Li, Z. Ma, Efficient and Secure Authentication Protocol for VANET, *2010 International Conference on Computational Intelligence and Security*, Nanning, China, 2010, pp. 523–527.

[18] J. Shao, X. Lin, R. Lu, C. Zuo, A Threshold Anonymous Authentication Protocol for VANETs, *IEEE Transactions on vehicular technology*, Vol. 65, No. 3, pp. 1711–1720, March, 2016.

[19] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, S. Gjessing, Mixgroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 13, No. 1, pp. 93–105, January-February, 2016.

[20] Y. Xi, K. Sha, W. Shi, L. Schwiebert, T. Zhang, Enforcing Privacy using Symmetric Random key- set in Vehicular Networks, *Eighth International Symposium on Autonomous Decentralized Systems*, Sedona, AZ, USA, 2007, pp. 344–351.

[21] P. Vijayakumar, M. Azees, A. Kannan, L. J. Deborah, Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, No. 4, pp. 1015–1028, April, 2016.

[22] A. Boualouache, S. Moussaoui, S2si: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs, *2014 International Conference on Advanced Networking Distributed Systems and Applications*, Bejaia, Algeria, 2014, pp. 70–75.

[23] B. Ying, D. Makrakis, Z. Hou, Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks, *IEEE Transactions on Vehicular Technology*, Vol. 64, No. 12, pp. 5631–5641, December, 2015.

[24] A. Boualouache, S.-M. Senouci, S. Moussaoui, Vlpz: The Vehicular Location Privacy Zone, *Procedia Computer Science*, Vol. 83, pp. 369–376, 2016.

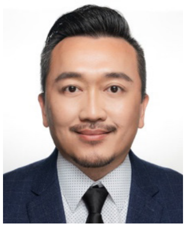
[25] V. G. Martinez, L. H. Encinas, S. Z. Song, Group Signatures in Practice, *Computational Intelligence Security for Information Systems Conference*, Burgos, Spain, 2015, pp. 413–423.

[26] Freeway Bereau, *Ministry of Transportation and Communications, Taiwan, Peak Traffic Flow of the Freeway in Taiwan*, https://1968.freeway.gov.tw/, 2023.

[27] Chungwha Telecomm, *Dr.Speed: Speedtest Tool Provides by Chungwa Telecom*, *https://speed.hinet. net/drspeed.html*.

Biographies

Nai-Wei Lo received the Ph.D. degrees in computer science and electrical engineering from the State University of New York at Stony Brook, Stony Brook, NY, USA, in 1998. He is a Professor with the Department of Information Management and the Dean of School of Management at National Taiwan University of Science and Technology in Taipei, Taiwan. His research interests include application and system security, IoT/IoV security, blockchain security, and cloud security. He is an associate editor of Journal of Information Security and Applications. He is a senior member of IEEE.



Chi-Ying Chuang received the M.S. degree in information management from the Chinese Culture University, Taipei, Taiwan, in 2012. In 2017, he received an M.S. degree in information management from the National Taiwan University, Taipei, Taiwan. He is currently pursuing his Ph.D. degree at the National Taiwan University of Science and Technology. His research interests include system security, privacy protection, and the Internet of Vehicles.

Jia-Ning Luo received the Ph.D. degree in computer science of National Chiao Tung University, Taiwan, in 2006. He is currently an associate professor of Department of Computer Science and Information Engineering, National Defense University, Taiwan. His research interests include network security, authentication protocols, the IoT security and eWallet security.

Chong-Long Yang received the M.S. degree in information management from National Taiwan University of Science and Technology, Taiwan, 2020.