

Article

RSU-Aided Remote V2V Message Dissemination Employing Secure Group Association for UAV-Assisted VANETs

Haowen Tan  and Ilyong Chung * 

Department of Computer Engineering, Chosun University, Gwangju 61452, Korea; tan_halloween@foxmail.com

* Correspondence: iyc@chosun.ac.kr; Tel.: +82-62-230-7712

Abstract: Nowadays, the research on vehicular ad hoc networks (VANETs) remains a hot topic within the Internet of Things (IoT) scenarios. Diverse studies and techniques regarding all aspects of VANETs have been investigated thoroughly. Particularly, the wireless characteristic of heterogeneous vehicular communication, along with the complicated and dynamic connection topology among participating VANET entities, have severely affected the secure and stable data exchange. Specifically, the spontaneous vehicle-to-vehicle (V2V) message dissemination, as the essential functionality of VANET, plays a significant role for instant and real-time data sharing for vehicles within a certain vicinity. However, with the short-time interaction and high mobilization of vehicular connections, the remote V2V message delivery intended for long-distance vehicles in the range of different roadside units (RSUs) has not been properly researched. Meanwhile, both V2V and V2R (Vehicle-to-RSU) communication are highly restricted by environmental factors such as physical obstructions or signal interferences, thus drastically reducing the wireless connectivity in practical VANET implementations. In this case, the unmanned aerial vehicles (UAVs), as the auxiliary facilities, can provide the VANET with substitute wireless routes, so that the transmission quality and availability can be improved. In this paper, the authenticated UAV group association design is proposed at first. On this basis, the remote V2V message dissemination method is enabled, where the decentralized V2V connections involving all RSUs along the way are provided. The analysis regarding crucial security properties is presented accordingly, where the formal proofs and comparison are conducted. Moreover, the performance evaluation in terms of storage and time consumption during RSU authentication process is illustrated, respectively. Comparison results with the state-of-the-art prove that superiority on the major performance factors can be achieved.



Citation: Tan, H.; Chung, I. RSU-Aided Remote V2V Message Dissemination Employing Secure Group Association for UAV-Assisted VANETs. *Electronics* **2018**, *10*, 548. <https://doi.org/10.3390/electronics10050548>

Academic Editor: Nurul I Sarkar

Received: 29 December 2020

Accepted: 22 February 2021

Published: 26 February 2021

Keywords: vehicular ad hoc networks (VANETs); unmanned aerial vehicles (UAVs); decentralized V2V communication; remote message dissemination; vehicular connectivity

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The tremendous popularization of the intelligent transportation system (ITS), which is considered to be the primary strategy for improving transportation quality, has been prompted by major enhancements in information and communication technology in recent years [1,2]. ITS, with its anticipated benefits, is responsible for delivering groundbreaking services and applications covering diverse modes of transport and traffic management, which are of particular interest to metropolitan cities and prosperous regions. Consequently, as the fundamental infrastructure of ITS, the VANET is characterized as the dispersed, self-organized wireless networks developed by heterogeneous vehicle entities. Generally, there are three key components of a typical VANET architecture: trusted authority (TA) as the centralized service provider, RSUs as the fundamental roadside facilities, and vehicles as the terminal users [3,4].

TA is in charge of the entire VANET operations including the confidential key allocation. Notably, vast vehicular data from VANET agencies are also consolidated and analyzed on the TA side. Evidently, TA is in strong need of computational and storage capabilities.

Nowadays, advanced networking and data transmission approaches, including promising 5G networks and cloud computing, have been devoted to a heterogeneous IoT paradigm including VANETs, where ample computing and storage capacity can be assured [5]. The remote cloud networks have been able to accommodate communications between several VANETs at the same time, accelerating the creation of a universal global vehicle internet initiative (IoV) [6]. The RSUs are specified as the dispersed facilities built along the road-sides at fixed intervals. The successful ranges of fixed RSUs are expected to cover all road areas in order to offer services to specified vehicles [7–9]. In particular, each RSU is able to perform the requisite key computing task and store critical data in its storage. Each vehicle can then at all times get access to the applications and resources from VANETs. As the terminal users of VANET, the vehicles in turn collaboratively collect vast heterogeneous vehicular data, as well as real-time road characteristics such as traffic congestion and car crash reports. The aggregated data are then transmitted to the VANETs central server for further processing. In the meantime, relevant VANETs services are being forwarded to those vehicles, which dramatically enhances driving safety. Functionally, each vehicle is installed with an on-board unit (OBU) on which wireless communication modules, including transceiver and transponder, are mounted [10–12]. The OBU of the vehicle is designed to manage both transmission and receiving of messages in the high-mobility environment.

Connectivity between the vehicle and its surrounding RSU can be accomplished by the communication between vehicle to RSU (V2R). Meanwhile, data exchange between vehicles can be assured by vehicle to vehicle connection (V2V). Self-organized wireless networks comprising multiple vehicles within specified locations can also be built [13,14], providing real-time data sharing and aggregation. Note that the dedicated short-range communications (DSRC) technique is implemented in both V2V and V2R communication. The interconnected system of VANETs is therefore developed with high connectivity and complex topology. However, critical V2V and V2R data sharing are carried out in the open wireless environment of realistic VANET circumstances. Therefore, serious vulnerability to various security threats and privacy risks exists [15,16]. The critical key details and user secrets may be unlawfully exposed to malicious attackers or unauthorized users, which may compromise the whole VANET network. In this case, efficient security preservation and privacy protection mechanisms in VANETs need to be deployed [17].

In practical VANET circumstances, the VANET data exchange is highly restrained by complicated physical environments and changeable communication conditions [18]. Specifically, the geographical barriers including high mountains and skyscrapers may obstruct the regular message delivery for V2V and V2R data sharing. Moreover, the dynamic wireless ad hoc topologies constructed by the spontaneous high-speed vehicles lead to a temporary and indisciplined interaction paradigm [19], which brings challenges to real-time V2V communication. In this case, the VANET connectivities will be drastically impacted, resulting in insufficient availability and low scalability. To address this practical issue, additional auxiliary facilities can be implemented in the VANET model for active connectivity improvement. Hence, multi-hop message forwarding can be provided with extra routes. With this motivation, the unmanned aerial vehicles (UAVs) can be applied to practical VANETs as the autonomous switching nodes for advancing the transmission quality and availability [20–22]. Apparently, with its unique advantages including substitutability, low expense, and applicability, the UAV-assisted VANETs could play a substantial part in practical VANET implementation [23]. In this case, the studies emphasizing UAV secure association and its correlation with the remaining VANET entities are imperative [24–26].

V2V communication provides instant and spontaneous data sharing channel for the nearby vehicles of comparatively short distances [27]. Therefore, open and legitimate data interactions among neighboring vehicles can be achieved, specifically for vehicles within one RSU domain. However, the V2V communication topology constructed by high-mobility vehicles may not properly satisfy the requirements for constant and reliable vehicular data exchange for long-distance vehicles. That is, due to the high mobility of participating vehicles, the constructed V2V network appears to be temporary and time-oriented [28]. For

example, two vehicles within one RSU domain can easily access the VANET and conduct V2V communication according to their own will. Both the V2V and V2R channels are securely preserved with advanced cryptographic techniques and strategies. However, the two vehicles are then traveling to different spots in the next moment, and each is in the range of individual RSU. At this moment, assuming the two vehicles have to disseminate subsequent messages, the conventional V2V communication intended for short-distance data exchange is not suitable. Meanwhile, the multi-hops channel among other vehicles is not efficient in this case. The long-distance remote V2V communications should be further studied accordingly. However, the corresponding remote V2V message delivery topic for long-distance vehicular communication in the range of different RSUs has not been properly researched so far.

Motivated by the above issues on secure VANET communication and V2V remote message dissemination, in this paper, the novel UAV-based VANET infrastructure is constructed initially. Therefore, VANET communication connectivity can be significantly improved, specifically for practical vehicular communication scenarios. Accordingly, the efficient group verification and key management process for the participating UAVs are presented. Moreover, the remote vehicular message dissemination for long-distance vehicles within different RSU domains is investigated. In the cross-domain authentication (CDA) paradigm, the decentralized V2V connection strategy with RSUs assistance is proposed.

1.1. Our Research Contributions

In this paper, the RSU-aided remote V2V message dissemination design with group association for UAV-assisted VANETs is proposed. The nontrivial efforts can be briefly summarized as follows:

- **Secure and efficient UAV association design with batch verification:** Our design adopts the UAV-assisted VANETs infrastructure, where multiple UAV entities are involved in V2V and V2R communications for connectivity improvement. The certificateless mutual authentication process for UAV association is developed. The partial secret key is utilized by the central server and UAV itself. Non-repudiation, user anonymity, and conditional privacy for each UAV can be guaranteed. Moreover, batch verification is provided in our design. Reliable vehicular data transmission in practical VANET environments can be achieved via the constructed UAV networks.
- **Dynamic key management and updating mechanism for UAV-assisted VANETs:** Upon verification, the corresponding UAV group key can be generated and safely distributed to the requesting UAVs. The efficient key updating method for all the involved UAVs is achieved. Notably, the dynamic UAV revocation is enabled, while the updated group key is timely acquired by the remaining legitimate UAVs. Heterogeneous vehicular data can then be forwarded through UAV assistance so that the geographic obstructions and interferences can be avoided with the alternative routes provided by UAV interactions.
- **RSU-aided remote V2V message dissemination with anonymity:** The remote vehicular data exchange method is presented for long-distance V2V communication. Particularly, the proposed design is conducted without remote cloud assistance. With the pre-stored driving records collected from the CDA process, the disseminated vehicular message can be forwarded through the edge RSUs and finally transmitted to the destination vehicle. Subsequently, anonymity for the participating vehicles can be guaranteed. Moreover, the superiority on both the security and performance characteristics can be achieved with the formal analysis and performance comparison.

The remainder of this paper is formulated as follows: The corresponding research development is briefly introduced in Section 2. To gain a better understanding of the topic, Section 3 outlines the requisite preliminary works and the developed UAV-assisted VANET system model. In Section 4, the secure UAV group authentication and key management, and V2V remote message dissemination are presented in detail. The security analysis

and performance discussion are presented in Section 5 and Section 6, respectively. The conclusions are drawn in Section 7.

2. Related Works

Nowadays, secure vehicular communication in VANET scenarios has been widely investigated. Various schemes on the authentication and key management for VANETs entities have been proposed so far. In 2012, to enhance privacy preservation and efficiency for key updating, Lu et al. [5] proposed the dynamic authenticated key management scheme with location-based services (LBSs) in VANETs. The double-registration detection mechanism is applied in the proposed DIKE scheme. The LBS session key is assigned to each time slot divided from LBS session. The backward secrecy can be achieved with the integrated threshold technique. Subsequently, the EMAP protocol intended for certificate revocation of VANET is developed in [18]. The received message is validated with the current certificate revocation lists (CRLs) for verifying the authenticity. Meanwhile, the generated keys for the related efficient revocation checking process are shared among the non-revoked vehicles. Subsequently, Lin et al. proposed an efficient cooperative authentication scheme for massive message validation in VANETs [9]. The authentication overhead for the individual vehicle can be reduced. Thereafter, the two-factor lightweight VANETs authenticating scheme (2FLIP) is designed by Wang et al. [4]. The decentralization of certificate authority (CA) and biological-password-based two-factor 2FA are applied. The lightweight hashing process with fast message authentication code (MAC) regeneration design is utilized for efficient user verification. The overhead of certificate management can be reduced with the decentralized CA structure. Similarly, Lo et al. developed the paring-free identity-based message authentication scheme with the batch signature mechanism [27], thus optimized performance in terms of time consumption can be achieved. Recently, several VANET authentication schemes emphasizing on lightweight vehicular verification and privacy-preserving have been developed [7,13].

As for secure V2V data exchange, Liu et al. proposed a dual authenticated key agreement scheme (PPDAS) for secure V2V communication in the IoV paradigm [19]. The historical vehicle trust reputation evaluation method is adopted for the final V2V session key establishment. The dual verification leverages anonymous vehicle identity and behavior authentication to improve decision-making accuracy. In the next, the decentralized lightweight authentication protocol for vehicular networks is developed in [2]. The biometric device (BD) and tamper-proof device (TPD) are used for vehicle verification and key preservation. The authentication signature protocol with hash-chain key generation is introduced for V2V interactions. Anonymous identities for vehicles are applied. Similarly, Wu et al. presented the privacy-preserving mutual authentication protocol for secure vehicular data exchange in dynamic topographical VANET scenarios [17]. Recent research also includes the V2V authentication method developed by Vasudev et al. [12].

The research on UAV communication has attracted lots of attention from academia. In 2017, Yoon et al. proposed the security authentication system employing the encrypted channel for UAV networks [24]. The hijacking problem for UAV control can be addressed. Subsequently, Zhou et al. developed the physical layer security improvement method through UAV with air-to-ground jammer for secure wireless communication [25]. In 2020, Gope et al. constructed the authenticated key agreement scheme for edge-assisted UAV networks. The mobile edge computing service providers are responsible for UAV verification in this scheme. In the next, Zhang et al. presented the gateway-oriented two-server authenticated key agreement [20]. The security of user passwords can be guaranteed in this way. Recently, a mobile edge computing (MEC) system with UAV assistance is developed in [23]. The ground users could offload the computing tasks to the nearby legitimate UAVs. Notably, the jamming signals are to be transmitted from the full-duplex legitimate UAV and other non-offloading ground users. The latency of the MEC system can be reduced accordingly. Aliev et al. proposed a scalable and lightweight group key management and matrix-based message encryption method for confidentiality preservation

of V2V broadcasting [22]. The distributed and scalable VANET architecture is applied. Overall, the existing V2V schemes mainly focus on the close vehicular communication within the single RSU domain, while the long-distance remote V2V communication has not been properly studied so far.

3. Preliminaries and Model Definitions

In this section, the relevant cryptographic principles and fundamental knowledge are presented in order to promote the reader's comprehension of the proposed schemes. The concepts of Lagrange polynomial interpolation, bilinear pairing, Chinese remainder theorem, and homomorphic encryption are introduced, respectively. Subsequently, the related notations, the UAV-assisted VANET system model, the security criteria, and network assumptions are defined.

3.1. Lagrange Polynomial Interpolation

Given a set of $k + 1$ different data points $\{(x_0, y_0), \dots, (x_j, y_j), \dots, (x_k, y_k)\}$, $\forall m \neq j$, $x_m \neq x_j$ holds. Define the polynomial of the degree k in a finite field $\mathbb{F}_p$ as $P_k(x) = a_0 + a_1x + \dots + a_kx^k$, where $a_i \in \mathbb{F}_p$ for $i \in \{0, \dots, k\}$. Hence, for $\forall i \in \{0, \dots, k\}$, $y_i = P_k(x_i)$ holds. The interpolation polynomial $L_k(x)$ in the Lagrange form can be defined as the linear combination as follows:

$$L_k(x) = \sum_{j=0}^k \ell_j(x) y_j.$$

Note that the Lagrange basis polynomials $\ell_j(x)$ ($0 \leq j \leq k$) are computed as

$$\ell_j(x) = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)} = \prod_{m=0, m \neq j}^k \frac{x - x_m}{x_j - x_m}.$$

That is, $L_k(x) = \sum_{j=0}^k \left(\prod_{m=0, m \neq j}^k \frac{x - x_m}{x_j - x_m} \right) y_j$ holds. Accordingly, for $\forall i \neq j$,

$$\begin{cases} \ell_j(x_i) = \prod_{m=0, m \neq j}^k \frac{x_i - x_m}{x_j - x_m} = \frac{(x_i - x_0)}{(x_j - x_0)} \cdots \frac{(x_i - x_{j-1})}{(x_j - x_{j-1})} \cdots \frac{(x_i - x_k)}{(x_j - x_k)} = 0 \\ \ell_j(x_j) = \prod_{m=0, m \neq j}^k \frac{x_j - x_m}{x_j - x_m} = 1 \end{cases}.$$

Hence, for the polynomial $P_k(x)$ of degree k , with $k + 1$ different data points on the graph of polynomial $P_k(x)$ and $L_k(x)$, the reconstruction of the polynomial $P_k(x)$ can be conducted accordingly.

3.2. Bilinear Pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the cyclic additive group and multiplicative group generated with the same prime order q . A mapping function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ can be defined as a bilinear pairing if all of the following three properties are satisfied:

1. *Bilinearity*: $\forall P, Q, R \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_q^*$, there is

$$\begin{cases} \hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} \\ \hat{e}(P, Q + R) = \hat{e}(Q + R, P) = \hat{e}(P, Q)\hat{e}(P, R) \end{cases}.$$

2. *Non-degeneracy*: $\exists P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
3. *Computability*: $\forall P, Q \in \mathbb{G}_1$, there is an efficient algorithm to calculate $\hat{e}(P, Q)$.

The bilinear map $\hat{e}$ satisfying the above properties can be constructed with the modified Weil pairing or Tate pairing on the supersingular elliptic curve $\mathbb{G}_1$, where the following characteristics are presented.

Definition 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)). Define $P, Q \in \mathbb{G}_1$, where $Q = aP$. Hence, for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, the advantage in finding the integer $a \in \mathbb{Z}_q^*$ to solve the ECDLP problem is defined as $\text{Adv}_{\mathcal{A}, \mathbb{G}_1}^{\text{ECDLP}}$, which is negligible as the following equation:

$$\text{Adv}_{\mathcal{A}, \mathbb{G}_1}^{\text{ECDLP}} = \Pr\left(\mathcal{A}(P, aP \in \mathbb{G}_1) \rightarrow a \mid \forall a \in \mathbb{Z}_q^*\right) \leq \varepsilon.$$

Definition 2 (Computational Diffie–Hellman Problem (CDHP)). Define $\mathbb{G}_1$ as the cyclic group with the large prime order q . Given $P, aP, bP \in \mathbb{G}_1$ for $a, b \in \mathbb{Z}_q^*$, where P is the generator of the cyclic group $\mathbb{G}_1$. Hence, for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, the advantage in finding computing abP for solving the given CDHP problem is defined as $\text{Adv}_{\mathcal{A}, \mathbb{G}_1}^{\text{CDHP}}$, which is negligible as the following equation:

$$\text{Adv}_{\mathcal{A}, \mathbb{G}_1}^{\text{CDHP}} = \Pr\left(\mathcal{A}(P, aP, bP \in \mathbb{G}_1) \rightarrow abP \in \mathbb{G}_1 \mid \forall a, b \in \mathbb{Z}_q^*\right) \leq \varepsilon.$$

3.3. Chinese Remainder Theorem (CRT)

Let $\{n_1, n_2, \dots, n_k\}$ be the pairwise co-prime positive integers. For an arbitrary sequence of integers $\{a_1, a_2, \dots, a_k\}$, the system congruences defined as

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a unique solution modulo $N = \prod_{i=1}^k n_i$. In this case, for $i = 1, 2, \dots, k$, we can get

$$\begin{cases} y_i = \frac{N}{n_i} = n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k \\ z_i \equiv y_i^{-1} \pmod{n_i} \end{cases}.$$

Hence, $y_i z_i \equiv 1 \pmod{n_i}$ and $y_j \equiv 0 \pmod{n_i}$ for $i \neq j$. The solution can be computed as

$$x = (a_1 y_1 z_1 + a_2 y_2 z_2 + \dots + a_k y_k z_k) \pmod{n_i} = \left(\sum_{i=1}^k a_i y_i z_i\right) \pmod{n_i}$$

3.4. Homomorphic Encryption

The homomorphic encryption design allows the predefined standard computations on ciphertexts, with which the output matches the encryption result on the computations conducted on plaintexts. With its unique properties, homomorphic encryption can be widely applied to vast security designs and privacy-preserving strategies. Hence, the transmitted data can be securely processed and out-sourced without revealing privacy-related information. The encryption and decryption functionalities can be considered as the homomorphisms between plaintext and ciphertext spaces. In practical communication scenarios with semi-trusted entities, homomorphic encryption could remove privacy barriers inhibiting data sharing since the operations on encrypted data can be performed instead of direct calculations on the confidential user data. The Paillier cryptosystem is one of the homomorphic cryptosystems for public key infrastructure (PKI). The security of Paillier cryptosystem is based on the decisional composite residuosity assumption (DCRA) described as follows:

Definition 3 (Decisional Composite Residuosity Assumption (DCRA)). Let p, q be two large primes such that $n = pq$. Given $\alpha \in \mathbb{Z}_{n^2}^*$, if there exist $\gamma \in \mathbb{Z}_{n^2}^*$ satisfying $\alpha \equiv \gamma^n \pmod{n^2}$, hence α is defined as the n -th residue modulo n^2 . Notably, given the composite n and an integer β , it is hard to decide whether β is the n -th residue modulo n^2 .

The Paillier encryption process is additively homomorphic. That is, the product of the two ciphertexts will decrypt to the sum of their corresponding plaintexts. Let $m_1, m_2 \in \mathbb{Z}_n^*$ be the plaintexts, $r_1, r_2, r_3 < n$ be the random integers during encryption. The following additive homomorphic properties can be satisfied:

$$\begin{cases} E(m_1, r_1) \cdot E(m_2, r_2) \bmod n^2 = E(m_1 + m_2, r_3) \bmod n \\ E(m_1, r_1)^\mu \bmod n^2 = E(m_1\mu, r_3) \bmod n \end{cases},$$

where $\mu \in \mathbb{Z}_n^*$ holds. $E(\cdot)$ denotes the encrypting operation.

3.5. Notations

The notations used in the proposed scheme, as well as the corresponding descriptions are listed in the following Table 1.

Table 1. Notations.

Symbol	Description
VC, RSUs	Vehicular Cloud, Road-Side Units
$\mathbb{G}_1, \mathbb{G}_2$	Cyclic Group
$\mathcal{G}$	Generator of $\mathbb{G}_1$
$\hat{e}$	Bilinear Pairing
$\mathfrak{t}_T^i, \mathfrak{t}_\perp^i$	RSU Identities
$\langle \mathfrak{s}_\perp^i, \mathfrak{r}_\perp^i \rangle$	Partial Secret Key Pair of RSU
$\mathfrak{t}_U^i, \mathfrak{t}_j^\otimes$	UAV Identities
$\langle \mathfrak{t}_j^\otimes, \mathfrak{r}_j^\otimes \rangle$	Partial Secret Key Pair of UAV
$\langle \mathcal{G}_i, \mathfrak{h}_i \rangle$	RSU Encryption Key Set
usk_j	UAV Session Key
gk^i	UAV Group Key
$\{\partial_i\}_{i \in [0, n]}$	Coefficients Set of $\mathbb{N}^i(x)$
$\mathfrak{t}_V^j, \mathfrak{t}_j$	Vehicle Identities
$\langle \mathfrak{t}_j, \mathfrak{r}_j \rangle$	Partial Secret Key Pair of Vehicle
$\langle \mathcal{X}_j, \xi_j \rangle$	Vehicle Encryption Key Pair
$\langle \mathcal{X}_j, \Gamma_j \rangle$	Vehicle Decryption Key Pair
$\langle H_1, H_2, H_3, H_4, H_5 \rangle$	Secure Hash Functions
$\langle h_1, h_2, h_3, h_4, h_5 \rangle$	Secure Hash Functions

3.6. System Model

The UAV-assisted VANET infrastructure of our design is briefly explained in this section. In our assumption, the UAVs participate in the vehicular communication process as the significant message forwarding and transmission node. The VANET wireless network connectivity can be improved in order to overcome the negative impacts caused by geographical obstructions and signal interferences. As shown in Figure 1, the typical VANETs system model consists of four different layers with distinctive functionalities: the vehicular

cloud as the central server, the edge layer containing the RSU facilities, the vehicle layer regarding the terminal vehicles/users, and the UAV layer for connectivity improvement. The relevant descriptions of the four VANET layers are respectively presented as follows.

Vehicular cloud is regarded as the core storage facility in charge of data storing and processing. Heterogeneous vehicular data of the whole VANET are analyzed in the vehicular cloud (VC). Notably, the utilized cloud architecture is able to provide sufficient processing and storage capabilities for multiple VANET prototypes simultaneously, which drastically facilitates the implementation of global IoV initiatives. Additionally, efficient data interchanges with nearby VANET facilities can be accomplished with the dedicated 5G communicating infrastructure. With full authority, the essential operations for the entire VANET system, including the vehicle registration, session key allocation, and user authentication, are all carried out by the VC, which is considered as the legitimate and trustworthy data server in the assumption. Note that VC is defined to be valid and trustworthy anytime.

Edge layer is defined as the distributed local VANET facility composed of various RSU clusters. Each RSU cluster maintains collaborative wired connections among the neighboring RSUs within the vicinity. Accordingly, the decentralized edge network for instant vehicular data exchange and service provision can be guaranteed. Each RSU cluster is responsible for essential vehicular information sharing and distributive edge computation. Overall, in the cloud-assisted VANET system, heterogeneous vehicular data are analyzed and stored in the cloud server, while the edge computing RSU clusters are deployed. Low latency, better response time, and transfer rates can be guaranteed in V2R interactions, which leverages the physical proximity to the terminal user. That is, the frequently used data requested from VC can be temporarily cached in the local edge server so that rapid response to the vehicles can be guaranteed. The bandwidth burden for VC can be significantly alleviated in this way.

Vehicle layer refers to the vehicle networks constructed during V2V and V2R communication. The embedded OBU within each vehicle is equipped with wireless transceiver and transponder for message delivery in high-mobility VANET scenarios. Meanwhile, the implemented TPD is for confidential information preservation. Notably, the vehicle, the OBU, and the driver are considered as one entity in our system model. Considering of the resource limitation, lightweight designs in terms of authentication and secure data exchange are crucial for practical VANETs.

UAV Cluster is defined as a set of autonomous switching nodes for advancing the transmission quality and availability. Upon validation, the legitimate UAV networks are responsible for the low-cost and multi-hop routing network construction. In practical VANET occasions, the geographical barriers such as high mountains and skyscrapers may interfere with regular V2V or V2R connections. In this case, the VANETs could take advantage of the self-organized UAV network and built substantial routing paths via dynamic UAV connections. Apparently, with its unique advantages including substitutability, low expense, and applicability, the UAV-assisted VANETs could play an imperative part in practical VANET implementation. The studies emphasizing UAV secure association and its correlation with the remaining VANET entities are vital.

3.7. Network Assumptions

As illustrated in Figure 1, the wired connections involving the VC and various local RSUs enable reliable vehicular data exchange with all the participating vehicles. Accordingly, effective strategies and techniques could be executed. Moreover, the connectivity between the vehicle and its surrounding RSU can be accomplished by V2R communication, while the data exchange between vehicles can be assured by V2V communication. All are supported by the dedicated short-range communications (DSRC) technique. However, critical V2V and V2R data sharing are carried out in the open wireless environment of realistic VANET circumstances. Therefore, serious vulnerability to various security threats and privacy risks exists. The critical key details and user secrets may be unlawfully exposed

to malicious attackers or unauthorized users, which may compromise the whole VANET network. In this case, efficient security preservation and privacy protection mechanisms in VANETs need to be deployed.

Additionally, the geographical barriers may also obstruct the regular message delivery for stable V2V and V2R data sharing. The dynamic wireless ad hoc topologies constructed by the spontaneous high-speed vehicles lead to a temporary and indisciplined interaction paradigm, which brings challenges to real-time V2V communication. In this case, the VANET connectivities will be drastically impacted, resulting in insufficient availability and low scalability. With this motivation, the unmanned aerial vehicles, as the additional auxiliary facilities, can be applied to practical VANETs as the autonomous switching nodes for advancing the transmission quality and availability. Hence, proper security methods are of significance for the interactions among UAVs and vehicles.

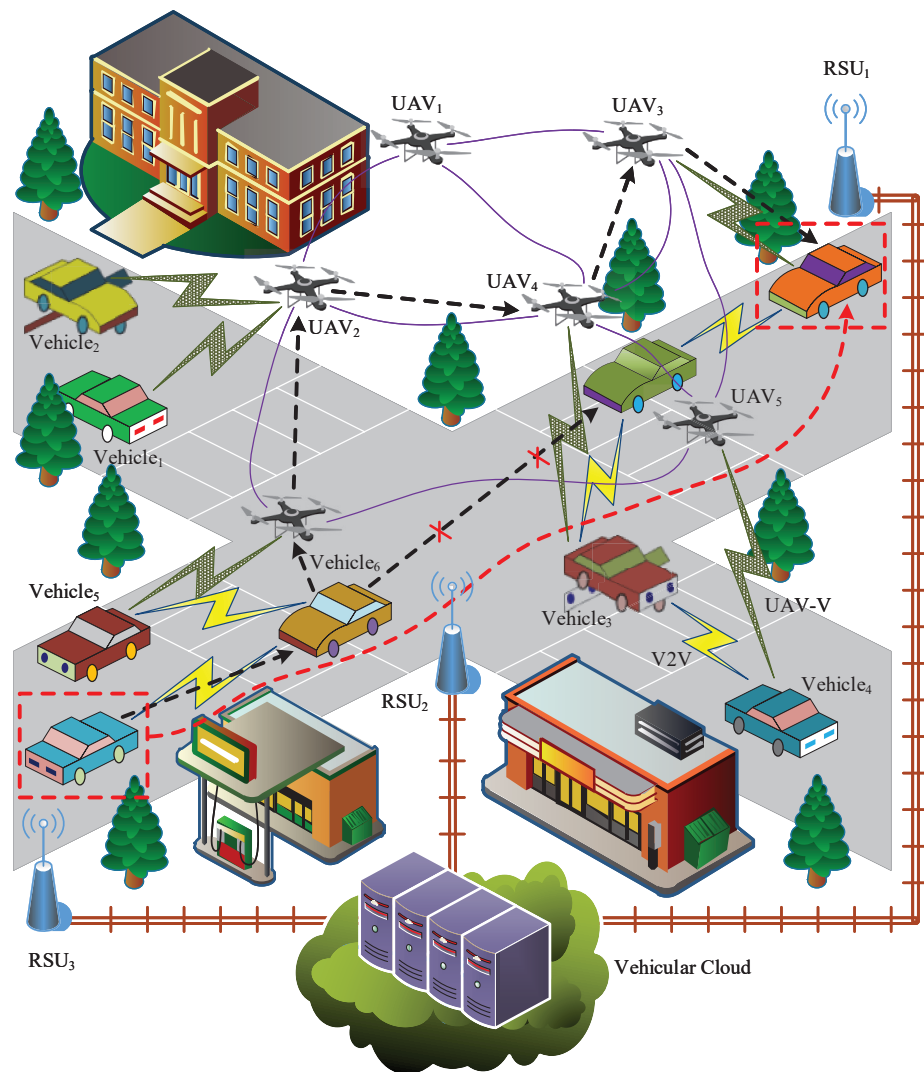


Figure 1. UAV-Assisted VANET System Model. The vehicles communicates with each other via V2V communication as shown with yellow lightening flash. The UAV-V communications are shown with ribbed lightening flash. The Vehicular Cloud maintains direct link with all RSUs. The neighboring UAVs associate with each other as shown with purple curve. The dotted red arrow indicates the remote V2V data delivery, which is conducted through the UAV-assisted VANET (dotted black arrow). In this way, the environmental obstructions can be avoided.

3.8. Security Objectives

The objectives of our design are to enhance the security assurance of UAV-assisted VANETs wireless transmissions and to address the remote V2V communication for long-distance, remote vehicles. The following security requirements for VAENT key management and authentication scheme should be fully satisfied:

- **Anonymity:** Messages originated from the same device carry unique patterns for verification of the receiver side. In the open wireless environment, by analyzing the eavesdropped information, vital parameters including the user location may be extracted, which endangers user privacy. Therefore, anonymity for all the participating vehicles during the whole VANET communications is extremely crucial.
- **Unforgeability:** The adversary may selectively forge the valid certificates, keys, or signatures in wireless VANET transmission in order to pass the verification process and acquire crucial system secrets. Unforgeability is the key property of safe data sharing against the selected message attack.
- **Session Key Establishment:** Upon validation, the shared session key between individual vehicles and the VANET system should be established so as to provide safe data exchange. Due to the semi-trustworthiness of intermediate RSUs, the constructed session key should be hidden from the interacting RSUs.
- **Conditional Privacy Preserving:** As one of the essential privacy criteria, conditional privacy is mainly composed of user privacy protection, and device identity retrieving. On the one hand, private information regarding user identity should be preserved during the entire transmission process. Hence, the illegal tracing toward the specific device cannot be performed. On the other hand, the legal authority should be capable of revealing the real identity of the individual vehicle under specific situations. The compromised or corrupted vehicle can then be timely traced.
- **Non-repudiation:** The message sender of VANET is unable to deny the authenticity of its signature on the messages transmitted. Non-repudiation guarantees that the information transmitted is valid.
- **Mutual Authentication:** Mutual authentication is the fundamental but leading security property in the VANET architecture, ensuring that the participating two VANET entities of the same communication session authenticate each other.

4. Proposed UAV Association and V2V Dissemination Scheme

In this section, the UAV authenticated key management scheme is developed, followed by the remote V2V message dissemination design. The proposed UAV group association design applies the certificateless cryptography technique for key escrow avoidance, where the partial secret key set is respectively managed by VC and individual UAV device. The user anonymity for the participating UAVs is provided accordingly. The edge RSU structure is responsible for pairing-based computations, while complicated processing tasks for resource-constrained UAVs are exempted during the whole process. Upon verification, the dynamic UAV group key distribution mechanism is conducted subsequently. Notably, efficient batch UAV validation design is enabled. In the next, the remote V2V message dissemination is presented. The RSU-aided vehicle communication is conducted through the RSU clusters along the driving path, while the vehicle route retrieving is achieved in this way.

The proposed scheme regarding UAV association can be roughly classified into the UAV batch authentication and group key distribution. In the initial UAV batch authentication, the UAV device registration and the nontrivial mutual verification design are executed. Subsequently, the universal group key is constructed for the universal UAV networks, which is of benefit to connectivity improvement in VANET implementation with geographical obstructions. Afterward, the remote V2V message delivery is composed of remote vehicular verification and V2V message dissemination, where the RSU-aided identity route retrieving method with remote VC assistance is developed.

4.1. UAV Batch Authentication

Initially, the corresponding UAV registration prior to the verification process is conducted, which is explicitly performed on the VC side. In this case, VC is in charge of vital UAV parameter allocation and essential key distribution to the destined UAVs. Firstly, $\mathbb{G}_1$ and $\mathbb{G}_2$ are respectively defined as the cyclic groups with the same large prime order q , where $\mathcal{G}$ denotes the generator of $\mathbb{G}_1$. Meanwhile, the map function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is defined as the bilinear pairing. The cryptographic hash functions $\{H_i\}_{i \in [1,5]}$ and $\{h_i\}_{i \in [1,5]}$ are respectively defined as $H_1 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_4 : \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_5 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_1 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_2 : \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_3 : \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $h_4 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_5 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. At this point, VC is able to generate the unique confidential secret set $\langle \mathfrak{t}_T^i, \mathfrak{s}_\perp^i \rangle$ for each validated RSU, where $\mathfrak{t}_T^i \in \{0,1\}^*$ denotes the identity, and $\mathfrak{s}_\perp^i \in \mathbb{Z}_q^*$ denotes the RSU partial secret key randomly generated by VC. At this moment, the confidential RSU information set $\langle \mathfrak{t}_T^i, \mathfrak{s}_\perp^i \rangle$ is safely shared among TA and each RSU itself.

Similarly, it is essential for each UAV to conduct the registration process in advance. The UAV identity $\mathfrak{t}_U^j \in \{0,1\}^*$ and the partial secret key $\mathfrak{t}_j^\otimes \in \mathbb{Z}_q^*$ are then assigned by VC. Hence, the key pair for UAV is defined as $\langle \mathfrak{t}_U^j, \mathfrak{t}_j^\otimes \rangle$. With the purpose of user anonymity preservation, each registered RSU randomly generates $\mathfrak{r}_\perp^i \in \mathbb{Z}_q^*$ and computes its temporary session identity $\mathfrak{t}_\perp^i$ as $\mathfrak{t}_\perp^i = h_1(\mathfrak{t}_T^i, \mathfrak{t}_T^i, \mathfrak{r}_\perp^i, \mathfrak{s}_\perp^i)$, where the current timestamp $\mathfrak{t}_T^i$ is adopted. In this case, each session identity $\mathfrak{t}_\perp^i$ is valid within a certain time interval. The partial secret key pair is stored as $\langle \mathfrak{r}_\perp^i, \mathfrak{s}_\perp^i \rangle$, while $\mathfrak{r}_\perp^i$ is kept secret to VC. Meanwhile, the homomorphic encryption design is utilized. That is, each RSU computes $\mathcal{G}_i = \mathcal{X}_i \mathcal{Y}_i$ satisfying $\gcd(\mathcal{X}_i \mathcal{Y}_i, (\mathcal{X}_i - 1)(\mathcal{Y}_i - 1)) = 1$, where $\mathcal{X}_i$ and $\mathcal{Y}_i$ denote the prime values randomly selected by RSU itself. Hence, RSU chooses random $\mathfrak{h}_i \in \mathbb{Z}_{\mathcal{G}_i}^*$ and computes $\mathfrak{A}_i = \text{lcm}(\mathcal{X}_i - 1, \mathcal{Y}_i - 1)$ and $\mathfrak{B}_i = \ell_i(\mathfrak{h}_i^{\mathfrak{A}_i} \bmod \mathcal{G}_i^2) \bmod \mathcal{G}_i$, where the function $\ell_i(x) = \frac{x-1}{\mathcal{G}_i}$. At this point, the RSU encryption key pair can be extracted as $\langle \mathcal{G}_i, \mathfrak{h}_i \rangle$. Subsequently, the following calculations are conducted by RSU

$$\begin{cases} \mathbb{J}^i = \mathfrak{r}_\perp^i \mathcal{G} \\ \mathbb{K}^i = \mathfrak{s}_\perp^i h_2(\mathfrak{t}_\perp^i, \mathfrak{r}_\perp^i) \mathcal{G} \\ \mathbb{R}^i = \mathfrak{r}_\perp^i \mathfrak{s}_\perp^i \mathcal{G} \\ \text{Sig}_\perp^i = H_1(\mathfrak{t}_N^i, \mathfrak{t}_\perp^i, \mathcal{G}_i, \mathfrak{h}_i, \mathbb{J}^i, \mathbb{K}^i, \mathbb{R}^i) \end{cases}, \quad (1)$$

where $\mathfrak{t}_N^i$ denotes the latest timestamp. At this point, the RSU parameters set $\langle \mathfrak{t}_N^i, \mathfrak{t}_\perp^i, \mathcal{G}_i, \mathfrak{h}_i, \mathbb{J}^i, \mathbb{K}^i, \mathbb{R}^i, \text{Sig}_\perp^i \rangle$ is published to all entities in its effective range. In the next, the UAV batch authentication process is described step by step. Assuming n UAVs with identity set $\langle \mathfrak{t}_U^j, \mathfrak{t}_j^\otimes \rangle$ ($j \in [1, n]$) are organized in the range of one RSU, and each UAV itself generates the partial secret key $\mathfrak{r}_j^\otimes \in \mathbb{Z}_q^*$ on its own. At this moment, the partial secret key pair $\langle \mathfrak{t}_j^\otimes, \mathfrak{r}_j^\otimes \rangle$ is stored in UAV storage. Hence, the temporary identity used in the authentication session is computed as $\mathfrak{t}_j^\otimes = H_2(\mathfrak{t}_U^j, \mathfrak{t}_j^\otimes, \mathfrak{r}_j^\otimes \mathcal{G})$. Meanwhile, all the UAVs are acknowledged of the published RSU parameters set $\langle \mathfrak{t}_N^i, \mathfrak{t}_\perp^i, \mathcal{G}_i, \mathfrak{h}_i, \mathbb{J}^i, \mathbb{K}^i, \mathbb{R}^i, \text{Sig}_\perp^i \rangle$. By validating the certificate $\text{Sig}_\perp^i$, the integrity of the received message can be guaranteed. Thereafter, each UAV computes

$$\begin{cases} \mathbb{S}_j = \mathfrak{r}_j^\otimes \mathcal{G} \\ \mathbb{T}_j = H_3(\mathfrak{t}_2^j, \mathfrak{t}_j^\otimes, \mathfrak{t}_\perp^i, \mathbb{S}_j) \end{cases} \quad (2)$$

and calculates the signature as $\Xi_j = H_4(\mathbf{r}_j^\otimes \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G} + \Upsilon_j[\mathbf{r}_j^\otimes \mathbb{K}^i + \mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathbb{J}^i]$, which combines the published RSU parameters with vehicle partial secret keys $\langle \mathbf{t}_j^\otimes, \mathbf{r}_j^\otimes \rangle$. The authentication requests $\langle Request, \mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbb{S}_j, \Upsilon_j, \Xi_j \rangle_{j \in [1, n]}$ from n vehicles are respectively delivered to RSU for further verification.

Upon receipt of the n requesting messages, the RSU checks the freshness of the received timestamp $\mathbf{t}_2^j$ and verifies Υ_j according to its session identity $\mathbf{t}_\perp^i$. Subsequently, RSU forwards $\langle \mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbb{S}_j \rangle$ to the VC for final identification. As mentioned above, significant identity information $\langle \mathbf{t}_U^j, \mathbf{t}_j^\otimes \rangle$ involving all the legitimate UAVs is stored in VC. Therefore, VC adopts the delivered $\mathbf{t}_2^j$ and $\mathbb{S}_j$ to the records and computes the UAV identity with the received one. If it matches, the identity of the UAV is confirmed. Hence, VC extracts the partial secret $\mathbf{t}_j^\otimes$ and computes $\Xi_j = \hat{e}(\mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G})$ and $\Xi_j = \hat{e}(H_4(\mathbf{t}_j^\otimes \mathbb{S}_j)\mathcal{G}, \mathcal{G})$, which will be forwarded to the RSU with session identity $\mathbf{t}_\perp^i$. At this moment, the confidential information set $\langle \Xi_j, \Xi_j, \Xi_j, \Upsilon_j, \mathbb{S}_j \rangle_{j \in [1, n]}$ for n UAVs are acquired by local RSU. Hence, RSU executes the following batch authentication calculation for n UAVs as

$$\frac{\hat{e}(\sum_{j=1}^n \Xi_j, \mathcal{G})}{(\prod_{j=1}^n \Xi_j)^{\mathbf{t}_\perp^i} \hat{e}(h_2(\mathbf{t}_\perp^i, \mathbf{r}_\perp^i)\mathcal{G}, \sum_{j=1}^n \Upsilon_j \mathbb{S}_j)^{\mathbf{t}_\perp^i}} \stackrel{?}{=} \prod_{j=1}^n \Xi_j. \quad (3)$$

The correctness of Equation (3) can be briefly elaborated as follows:

$$\begin{aligned} & \frac{\hat{e}(\sum_{j=1}^n \Xi_j, \mathcal{G})}{(\prod_{j=1}^n \Xi_j)^{\mathbf{t}_\perp^i} \hat{e}(h_2(\mathbf{t}_\perp^i, \mathbf{r}_\perp^i)\mathcal{G}, \sum_{j=1}^n \Upsilon_j \mathbb{S}_j)^{\mathbf{t}_\perp^i}} \\ &= \frac{\prod_{j=1}^n \hat{e}(\Upsilon_j \mathbf{r}_j^\otimes \mathbb{K}^i, \mathcal{G}) \hat{e}(\sum_{j=1}^n \Upsilon_j \mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathbb{J}^i, \mathcal{G}) \hat{e}(\sum_{j=1}^n H_4(\mathbf{r}_j^\otimes \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G})}{(\prod_{j=1}^n \Xi_j)^{\mathbf{t}_\perp^i} \hat{e}(h_2(\mathbf{t}_\perp^i, \mathbf{r}_\perp^i)\mathcal{G}, \sum_{j=1}^n \Upsilon_j \mathbf{r}_j^\otimes \mathcal{G})^{\mathbf{t}_\perp^i}} \\ &= \frac{\prod_{j=1}^n \hat{e}(\Upsilon_j \mathbf{r}_j^\otimes \mathbb{K}^i, \mathcal{G}) \hat{e}(\sum_{j=1}^n \Upsilon_j \mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathbb{J}^i, \mathcal{G}) \hat{e}(\sum_{j=1}^n H_4(\mathbf{r}_j^\otimes \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G})}{\prod_{j=1}^n \hat{e}(\mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G})^{\Upsilon_j \mathbf{t}_\perp^i} \hat{e}(\sum_{j=1}^n \Upsilon_j \mathbf{r}_j^\otimes \mathbb{K}^i, \mathcal{G})} \\ &= \frac{\hat{e}(\sum_{j=1}^n \Upsilon_j \mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathbb{J}^i, \mathcal{G}) \prod_{j=1}^n \hat{e}(H_4(\mathbf{r}_j^\otimes \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G})}{\hat{e}(\sum_{j=1}^n \Upsilon_j \mathbf{t}_j^\otimes H_2(\mathbf{t}_2^j, \mathbf{t}_j^\otimes, \mathbf{t}_j^\otimes \mathcal{G})\mathbb{J}^i, \mathcal{G})} \\ &= \prod_{j=1}^n \hat{e}(H_4(\mathbf{r}_j^\otimes \mathbf{t}_j^\otimes \mathcal{G})\mathcal{G}, \mathcal{G}) \\ &= \prod_{j=1}^n \Xi_j \end{aligned} \quad (4)$$

The batch authentication process involving n UAVs is performed in this way. Therefore, if the request message does not pass the validation process, the current authentication session is terminated. Otherwise, for the n UAVs, RSU computes $\mathbf{t}_j^\dagger = h_2(\mathbf{t}_j^\otimes, H_4(\mathbf{r}_\perp^i \mathbb{S}_j))$ and $Sig_j^\dagger = H_3(\mathbf{t}_3^j, \mathbf{t}_\perp^i, \mathbf{t}_j^\dagger, \Xi_j)$ and distributes the acknowledgment message $\langle \mathbf{t}_3^j, \mathbf{t}_j^\dagger, Sig_j^\dagger \rangle_{j \in [1, n]}$, where $\mathbf{t}_3^j$ denotes the latest timestamp.

Upon receiving the acknowledgement message, UAV first checks the freshness of $\mathbf{t}_3^j$ and then validates the correctness of $\mathbf{t}_j^\dagger$ and $Sig_j^\dagger$ according to $\mathbf{t}_j^\dagger = h_2(\mathbf{t}_j^\otimes, H_4(\mathbf{r}_\perp^i \mathbb{S}_j)) = h_2(\mathbf{t}_j^\otimes, H_4(\mathbf{r}_j^\otimes \mathbb{J}^i))_{j \in [1, n]}$. Note that the current UAV identity is now updated as $\mathbf{t}_j^\dagger$ to provide message unlinkability. At this point, mutual authentication among UAVs and

RSU is provided, which adopts the certificateless cryptographic technique for key escrow avoidance. The partial secret keys of individual UAV are respectively generated by VC and UAV itself. Moreover, bilinear pairing is utilized, while the complicated pairing calculations are exempted in UAV sides. In our design, the shared session key $usk_j^\otimes$ for the individual UAV is independently constructed as $usk_j^\otimes = H_4(\Xi_j)$, which can be used for the following UAV group key distribution process.

4.2. Group Key Distribution

The group key involving all the n validated UAVs is distributed in each RSU domain so that the substantial UAV networks can be built. Initially, for $j \in [1, n]$, RSU computes $\sigma_j = \frac{1}{usk_j^\otimes} (\prod_{i=1}^n usk_i^\otimes)$ and $\mu_j \equiv \sigma_j^{-1} \bmod usk_j^\otimes$ satisfying $\mu_j \sigma_j = 1 \bmod usk_j^\otimes$ for $\forall j \in [1, n]$. In the next, RSU chooses the distinctive UAV group key $gk^i \in \mathbb{Z}_q^*$ and extracts the keying value as $\tau^i = gk^i \sum_{j=1}^n (\mu_j \sigma_j)$. At this point, the keying function can be constructed in the form of $\aleph^i(x) = gk^i \sum_{j=1}^n (\mu_j \sigma_j) + \prod_{j=1}^n (x - usk_j^\otimes)$, which can be further transformed into $\aleph^i(x) = \sum_{j=0}^n \partial_j x^j$. Notably, the corresponding coefficients set $\{\partial_0, \dots, \partial_n\}$ is extracted. Therefore, $\forall \ell \in [1, n]$, $\aleph^i(usk_\ell^\otimes) = gk^i \sum_{j=1}^n (\mu_j \sigma_j) + \prod_{j=1}^n (usk_\ell^\otimes - usk_j^\otimes) = gk^i \sum_{j=1}^n (\mu_j \sigma_j)$ holds. Hence, the following computation is conducted as $Sig_{gk}^i = h(\mathfrak{t}_{gk}^i, \mathfrak{t}_\perp^i, \partial_0, \dots, \partial_n, gk^i \sum_{j=1}^n (\mu_j \sigma_j))$, where $h(\cdot)$ denotes the secure hash function. Accordingly, RSU broadcasts the keying packet as $\langle \mathfrak{t}_{gk}^i, \mathfrak{t}_\perp^i, \{\partial_j\}_{j \in [0, n]}, Sig_{gk}^i \rangle$. Finally, all the n UAVs receive the keying packet and reconstruct the function $\aleph^i(x)$ so that the group key gk^i can be correctly derived as $gk^i = \aleph^i(usk_j^\otimes) \bmod usk_j^\otimes$. In this way, the UAV group key is shared among all requesting n UAVs.

4.3. Remote Vehicular Verification

In this section, the V2V communication assumptions are presented at first. As shown in Figure 2, assuming at timepoint t_1 , the vehicles V_1 and V_2 are in the range of original RSU_1 , the instant V2V interactions between V_1 and V_2 can be achieved through multiple existing schemes so far [19,22,29]. At the current time t_2 ($t_2 > t_1$), both V_1 and V_2 are now arriving at different RSU domains. At this moment, the $V_1 \rightarrow V_2$ vehicular connection is required in the case for the subsequent message dissemination, which has not been properly addressed in the existing VANET schemes. Therefore, the remote vehicular verification is introduced in this section, followed by the remote V2V message dissemination in the next section.

Initially, assuming the vehicle with original identity $\mathfrak{t}_V^j$ and that the partial secret key pair $\langle \mathfrak{t}_j, \mathfrak{r}_j \rangle$ is approaching the communicating range of specific RSU, its temporary identity can be updated as $\mathfrak{t}_j = h_3(\mathfrak{t}_V^j, \mathfrak{r}_j \mathcal{G})$. Meanwhile, the vehicle extracts the encryption key pair $\langle \mathcal{G}_i, \mathfrak{h}_i \rangle$ from the published $\langle \mathfrak{t}_N^i, \mathfrak{t}_\perp^i, \mathcal{G}_i, \mathfrak{h}_i, \mathbb{J}^i, \mathbb{K}^i, \mathbb{R}^i, Sig_\perp^i \rangle$. Following the same way as that of the RSU, the vehicle homomorphic encryption design with encryption key pair $\langle \mathcal{X}_j, \xi_j \rangle$ and decryption key pair $\langle \mathcal{X}_j, \Gamma_j \rangle$ is constructed. Therefore, the vehicle calculates $Sig_V^j = \mathfrak{h}_i^{(\mathfrak{x}_j || \mathcal{X}_j, \xi_j || \mathfrak{f}_j)} \cdot \mathfrak{r}_j^{\mathcal{G}_i} \bmod \mathcal{G}_i^2$, with

$$\begin{cases} \mathfrak{f}_j = \mathfrak{r}_j \mathbb{R}^i \\ \mathfrak{x}_j = H_2(\mathfrak{t}_\circ^j, \mathfrak{t}_V^j, \mathfrak{t}_j \mathfrak{r}_j \mathcal{G}) \\ \mathfrak{f}_j = H_5(\mathfrak{t}_\circ^j, \mathfrak{t}_j, \mathbb{R}^i, \mathcal{X}_j, \xi_j, \mathfrak{x}_j) \end{cases}, \quad (5)$$

and sends the requesting packet $\langle \text{Request}, \mathfrak{t}_\circ^j, \mathfrak{t}_j, \mathfrak{f}_j, Sig_V^j \rangle$ to RSU for further verification.

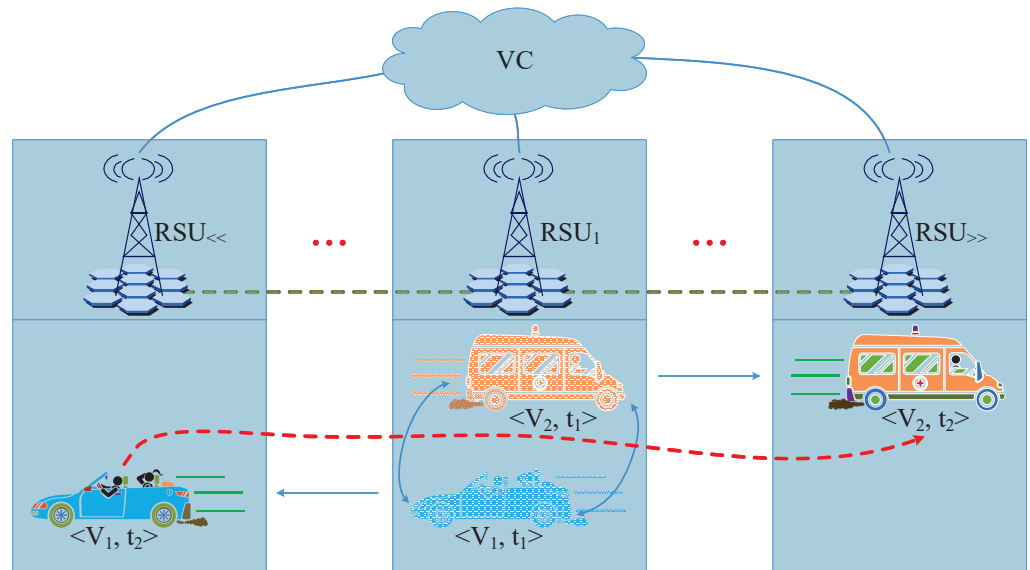


Figure 2. RSU-aided remote V2V message dissemination.

Upon receipt of the packet, RSU decrypts the received Sig_V^j using the decryption key $\langle \mathcal{G}_i, \mathcal{A}_i \rangle$ and then extracts $\langle \mathcal{X}_j || \mathcal{X}_j, \xi_j || \mathfrak{F}_j \rangle$. If the values of $\mathfrak{F}_j$ and $\mathcal{X}_j$ are validated, RSU stores the vehicle homomorphic encryption key pair $\langle \mathcal{X}_j, \xi_j \rangle$. Moreover, the value $\mathfrak{N}_j$ can be calculated as $\mathfrak{N}_j = (\mathfrak{r}_\perp^i s_\perp^i)^{-1} \mathfrak{S}_j = \mathfrak{r}_j \mathcal{G}$. At this point, RSU uploads $\langle \mathfrak{t}_o^j, \mathfrak{F}_j, \mathfrak{N}_j, \mathcal{X}_j \rangle$ to VC for remote identification. Thereafter, VC computes $\mathfrak{D}_j = h_3(\mathfrak{F}_V^j, \mathfrak{t}_j \mathfrak{r}_j \mathcal{G})$ and replies to RSU with the acknowledgment $\langle Ack, \mathfrak{F}_j, \mathfrak{D}_j \rangle$. Subsequently, RSU updates the vehicle identity as $\mathfrak{F}_j^1 = h_3(\mathfrak{F}_j, \mathfrak{r}_\perp^i s_\perp^i \mathcal{G})$, where the RSU key pair $\langle \mathfrak{r}_\perp^i, s_\perp^i \rangle$ is adopted. Note that, in our design, anonymous identity of the participating vehicle is safely updated as soon as a verification session is finished successfully. In this case, the message unlinkability for different communication sessions can be guaranteed. Untraceability of specific vehicle is provided as well.

With the aforementioned vehicle key pair $\langle \mathcal{X}_j, \xi_j \rangle$ and its own $\mathfrak{r}_\perp^i$, RSU conducts the vehicle homomorphic encryption process and computes $Sig_\perp^j = \xi_j^{\mathfrak{D}_j} \cdot (\mathfrak{r}_\perp^i)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2$ and $\Phi_j = h_1(\mathfrak{t}_o^j, \mathfrak{F}_j^1, Sig_\perp^j)$. Hence, RSU is able to broadcast the packet $\langle \mathfrak{t}_o^j, \mathfrak{F}_j^1, Sig_\perp^j, \Phi_j \rangle$ to the destined vehicle. Upon validation on the timestamp $\mathfrak{t}_o^j$, the vehicle is able to decrypt the received $Sig_\perp^j$ and successfully extract $\mathfrak{D}_j$. Notably, Φ_j of the delivered packet is for integrity validation. Therefore, the vehicle extracts the final verification process as $\mathfrak{D}_j \stackrel{?}{=} h_3(\mathfrak{F}_V^j, \mathfrak{t}_j \mathfrak{r}_j \mathcal{G})$. At this point, the vehicle validation with the original RSU is completed. The session key established between VC and vehicle is generated as $sk_j = H_4(\mathfrak{t}_j \mathfrak{r}_j \mathcal{G})$, which can be used as the unique identifier between vehicle and VC. Meanwhile, the unique proof for each validated vehicle is issued as $\mathfrak{P}_{[j,1]}^\prec = Sig_\perp^j \cdot \xi_j^{h_2(\mathfrak{F}_\perp^i, \mathfrak{S}_j)} \cdot (\mathfrak{r}_\perp^i)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2$, where $\mathfrak{r}_\perp^i \in \mathbb{Z}_q^*$ ($\mathfrak{r}_\perp^i \neq \mathfrak{r}_\perp^i$) is the newly generated pseudorandom for remote vehicle verification. Moreover, the relevant certificate is computed as $Sig_{[j,1]}^\infty = h_4(\mathfrak{F}_j^1, \mathcal{X}_j, \xi_j, \mathfrak{P}_{[j,1]}^\prec)$. In this case, the original RSU will deliver the packet $\langle \mathfrak{F}_j^1, \mathcal{X}_j, \xi_j, \mathfrak{P}_{[j,1]}^\prec, Sig_{[j,1]}^\infty \rangle$ to all its neighboring RSUs via the edge networks. Upon receiving the packet, all its neighboring RSUs temporarily store it in their storage for possible further use. If not required in a certain time interval Δ_α , the packet will be abandoned.

In our assumption, the vehicle is on the path of $RSU_1 \rightarrow RSU_n$. Hence, in the domain of RSU_2 with RSU parameter set $\langle t_N^i, \mathbb{P}_\perp^i, \mathcal{G}_i, h_i, \mathbb{J}^i, \mathbb{K}^i, \mathbb{R}^i, Sig_\perp^i \rangle$, the vehicle randomly generates $\tau_j^\alpha \in \mathbb{Z}_q^*$ and computes

$$\begin{cases} \mathbb{P}_{[j,1]}^\prec = \zeta_j^{(\bar{\theta}_j - h_2(\mathbb{P}_\perp^i, \mathbb{S}_j))} \cdot (\tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \\ \mathbb{U}_{[j,1]} = h_5 \left(\zeta_j^{2\bar{\theta}_j} \cdot (\tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \end{cases} \quad (6)$$

Subsequently, the vehicle conducts the RSU encryption using the broadcast key $\{\mathcal{G}_2, h_2\}$ of RSU_2 as

$$Sig_{[j,1]}^\boxtimes = h_2 \left(\mathbb{P}_{[j,1]}^\prec, \tau_j^\alpha \mathcal{G}, \mathbb{P}_{[j,1]}^\prec, \mathbb{U}_{[j,1]} \right) \cdot (\tau_j^\alpha)^{\mathcal{G}_2} \bmod \mathcal{G}_2^2, \quad (7)$$

which will be delivered to RSU_2 for fast verification.

Upon receiving $Sig_{[j,1]}^\boxtimes$, RSU_2 is able to decrypt it and extract $\langle \mathbb{P}_{[j,1]}^\prec, \tau_j^\alpha \mathcal{G}, \mathbb{P}_{[j,1]}^\prec, \mathbb{U}_{[j,1]} \rangle$. Notably, RSU_2 has already received $\langle \mathbb{P}_{[j,1]}^\prec, \mathcal{X}_j, \zeta_j, \mathbb{P}_{[j,1]}^\prec, Sig_{[j,1]}^\alpha \rangle$ from the original RSU_1 . Therefore, the validation $h_5(\mathbb{P}_{[j,1]}^\prec \cdot \mathbb{P}_{[j,1]}^\prec) \stackrel{?}{=} \mathbb{U}_{[j,1]}$ could be executed. The correctness can be elaborated as

$$\begin{aligned} & h_5(\mathbb{P}_{[j,1]}^\prec \cdot \mathbb{P}_{[j,1]}^\prec) \\ &= h_5 \left(Sig_\perp^i \cdot \zeta_j^{h_3(\mathbb{P}_\perp^i, \mathbb{S}_j)} \cdot (\tau_i^\perp)^{\mathcal{X}_j} \cdot \zeta_j^{(\bar{\theta}_j - h_3(\mathbb{P}_\perp^i, \mathbb{S}_j))} \cdot (\tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \\ &= h_5 \left(\zeta_j^{\bar{\theta}_j} \cdot (\tau_i^\perp)^{\mathcal{X}_j} \cdot \zeta_j^{h_3(\mathbb{P}_\perp^i, \mathbb{S}_j)} \cdot (\tau_i^\perp)^{\mathcal{X}_j} \cdot \zeta_j^{(\bar{\theta}_j - h_3(\mathbb{P}_\perp^i, \mathbb{S}_j))} \cdot (\tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \\ &= h_5 \left(\zeta_j^{\bar{\theta}_j + \bar{\theta}_j - h_3(\mathbb{P}_\perp^i, \mathbb{S}_j) + h_3(\mathbb{P}_\perp^i, \mathbb{S}_j)} \cdot (\tau_i^\perp \cdot \tau_i^\perp \cdot \tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \\ &= h_5 \left(\zeta_j^{2\bar{\theta}_j} \cdot (\tau_i^\perp \cdot \tau_i^\perp \cdot \tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \\ &= h_5 \left(\zeta_j^{2\bar{\theta}_j} \cdot (\tau_j^\alpha)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \right) \\ &= \mathbb{U}_{[j,1]} \end{aligned} \quad (8)$$

At this point, the current identity $\mathbb{P}_j^1$ and the previous received $\mathbb{P}_{[j,1]}^\prec$ should be updated as $\mathbb{P}_j^2 = h_3(\mathbb{P}_j^1, \tau_j^\alpha \mathcal{G})$ and $\mathbb{P}_{[j,2]}^\prec = \mathbb{P}_{[j,1]}^\prec \mathbb{P}_{[j,1]}^\prec Enc_{\langle \mathcal{X}_j, \zeta_j \rangle}^{\tau_i^\perp} \left[h_3(\mathbb{P}_\perp^i, \tau_j^\alpha \mathbb{R}^2) \right]$. In this case, RSU_2 computes the certificate information for final authentication on the vehicle side, which is encrypted with vehicle homomorphic encryption key pair $\langle \mathcal{X}_j, \zeta_j \rangle$ and the generated pseudorandom $\tau_i^\perp \in \mathbb{Z}_q^*$ as $Sig_2^F = Enc_{\langle \mathcal{X}_j, \zeta_j \rangle}^{\tau_i^\perp} \left[\mathbb{P}_{[j,1]}^\prec \mathbb{P}_{[j,1]}^\prec || h_1(t_\alpha^2, \mathbb{P}_j^2, \mathbb{P}_{[j,1]}^\prec, \mathbb{P}_{[j,1]}^\prec) \right]$, where t_α^2 is the current timestamp for authentication. The packet $\langle t_\alpha^2, \mathbb{P}_j^2, Sig_2^F \rangle$ is then sent to the vehicle for mutual verification. Upon receiving $\langle t_\alpha^2, \mathbb{P}_j^2, Sig_2^F \rangle$, the vehicle derives $\langle \mathbb{P}_{[j,1]}^\prec \mathbb{P}_{[j,1]}^\prec || h_1(t_\alpha^2, \mathbb{P}_j^2, \mathbb{P}_{[j,1]}^\prec, \mathbb{P}_{[j,1]}^\prec) \rangle$ to confirm the identity of RSU_2 .

4.4. V2V Message Dissemination

In the assumption, in further time t_2 of the n cross-domain verification sessions, $\langle \ddagger_j^n, \mathcal{X}_j, \xi_j, \mathfrak{P}_{[j,n]}^\prec, \text{Sig}_{[j,n]}^\alpha \rangle$ will be broadcast by RSU_n , where

$$\begin{cases} \ddagger_j^n = h_3(\ddagger_j^{n-1}, \mathfrak{r}_j^\alpha \mathcal{G}) \\ \mathfrak{P}_{[j,n]}^\prec = \mathfrak{P}_{[j,n-1]}^\prec \mathfrak{P}_{[j,n-1]}^\succ \xi_j^{h_2(\ddagger_{\perp}^n, \mathfrak{r}_j^\alpha \mathbb{R}^n)} \cdot (\mathfrak{r}_n^\perp)^{\mathcal{X}_j} \bmod \mathcal{X}_j^2 \end{cases} \quad (9)$$

Intuitively, the anonymous identity for each vehicle is updated in each session. The $\mathfrak{P}_{[j,k]}^\prec$ is also updated based on the previously validated proofs and the keys from the current RSU_n . As mentioned above, each RSU around the path safely preserves the identities, valid proofs, and the corresponding timestamps for all the passing-by legitimate vehicles. The remote long-distance V2V message dissemination method can be constructed accordingly.

Assuming a vehicle V_1 intends to conduct remote vehicular data exchange with the vehicle V_2 at time t_2 , V_1 is in the range of $RSU_{\ll}$, V_2 is in the range of $RSU_{\gg}$. Notably, both V_1 and V_2 crossed the original RSU_1 previously and conducted V2V communication at t_1 ($t_2 > t_1$). In this case, assuming the vehicle V_2 is with original identity $\ddagger_V^2$ and the partial secret key pair $\langle \mathfrak{t}_2, \mathfrak{r}_2 \rangle$, the two historical temporary identities in the range of RSU_1 are $\ddagger_2 = h_3(\ddagger_V^2, \mathfrak{r}_2 \mathcal{G})$ and $\ddagger_1^1 = h_3(\ddagger_2, \mathfrak{r}_1^\perp s_1^\perp \mathcal{G})$. The vehicle V_1 is able to retrieve the $\langle \ddagger_2, \ddagger_1^1 \rangle$ from its historical transmission record. In this case, the current $RSU_{\ll}$ broadcast $\langle \mathfrak{t}_N^{\ll}, \ddagger_{\perp}^{\ll}, \mathcal{G}_{\ll}, \mathfrak{h}_{\ll}, \mathbb{J}_{\ll}, \mathbb{K}_{\ll}, \mathbb{R}_{\ll}, \text{Sig}_{\perp}^{\ll} \rangle$ to all. In the meantime, the current identity of vehicle V_1 is $\ddagger_1^{\ll} = h_3(\ddagger_1^{\ll-1}, \mathfrak{r}_1^\alpha \mathcal{G})$. The vehicle generates the packet to be delivered as $\langle \mathfrak{t}_1^\nabla || \ddagger_1^{\ll} || \mathcal{P}_1^{\ll} || h_1(\mathfrak{t}_1^\nabla, \ddagger_1^{\ll}, \mathcal{P}_1^{\ll}) \rangle$, where $\mathcal{P}_1^{\ll} = \mathfrak{h}_{\ll}^{\mathfrak{t}_1^\nabla || \ddagger_1^{\ll} || sk_1 || \mathcal{M} || \ddagger_2 || \mathfrak{t}_2^\Delta} \cdot \mathfrak{r}_1^{\mathcal{G}_{\ll}} \bmod \mathcal{G}_{\ll}^2$. Respectively, $\mathfrak{t}_1^\nabla$ and $\mathfrak{t}_2^\Delta$ denote the current timestamp generated on vehicle V_1 , and the previous timestamp associated with time t_1 . $\ddagger_2$ refers to the temporary identity previous used by the destined vehicle V_2 at t_1 . The identifier sk_1 is adopted for distinction on $RSU_{\ll}$. $\mathcal{M}$ refers to the confidential data intended to be sent.

The current $RSU_{\ll}$ then decrypts the packet and derives $\mathcal{P}_1^{\ll}$ after validation on $\mathfrak{t}_1^\nabla$ and $h_3(\mathfrak{t}_1^\nabla, \ddagger_1^{\ll}, \mathcal{P}_1^{\ll})$. Notably, the vehicle V_1 has already passed the cross-domain validation process conducted by $RSU_{\ll}$. Therefore, the corresponding identity $\ddagger_1^{\ll-1} = h_3(\ddagger_1^{\ll-2}, \mathfrak{r}_1^\alpha \mathcal{G})$ acquired from $RSU_{\ll-1}$ is also stored in $RSU_{\ll}$ side. The packet is then forwarded to the previous RSUs following the sequence of $\langle RSU_{\ll}, RSU_{\ll-1}, \dots, RSU_1 \rangle$. Each RSU in the sequence holds the record of vehicle V_1 on $\langle \ddagger_1^i, \ddagger_1^{i-1} \rangle$ ($i \in [1, \ll]$). The remote V2V packet can then be delivered to the original RSU_1 . Subsequently, RSU_1 extracts the $\langle \ddagger_2, \ddagger_1^1 \rangle$ record of V_2 and continues broadcasting the packet to neighboring RSUs. Each RSU holds the record of vehicle V_2 on $\langle \ddagger_2^i, \ddagger_2^{i-1} \rangle$ ($i \in [1, \gg]$). Finally, the message $\mathcal{M}$ can be delivered to V_2 by $RSU_{\gg}$. The remote V2V message dissemination process is completed.

5. Security Analysis

In this section, the crucial security properties described in the previous Section 3.8 are analyzed in order to demonstrate the proposed scheme is provably secure. Moreover, the security comparisons on the major characteristics with the state-of-the-art are shown.

5.1. Security Discussions

Definition 4 (Forking Lemma [30]). Define $\mathcal{A}$ as the probabilistic polynomial-time Turing machine with only the public data as input. With non-negligible probability, $\mathcal{A}$ can generate a valid signature $(m, \delta_1, \delta_2, h)$ within a certain time bound $\mathbb{T}$, where the tuple (δ_1, δ_2, h) is simulated without accessing the secrets. In this case, with an indistinguishable distribution probability, there is another machine that has control over the machine obtained from $\mathcal{A}$ replacing interaction with the signer by simulation and produces two valid signatures $(m, \delta_1, \delta_2, h)$ and $(m, \delta_1, \delta_2', h')$ ($h \neq h'$).

Theorem 1. *The proposed scheme is provably unforgeable towards CMA if the CDHP is intractable.*

Proof of Theorem 1. Initially, let $\mathcal{A}_1$ be a probabilistic polynomial time (PPT) adversary who could violate the proposed authentication scheme with a non-negligible advantage. The challenger $\mathcal{C}_1$ is constructed to solve the CDHP with a non-negligible advantage. According to Definition 4, within a polynomial time, adversary $\mathcal{A}_1$ obtains two validated signatures $\langle \mathfrak{t}_j^\otimes, \mathfrak{r}_j, \mathfrak{z}_j, \mathfrak{E}_j, \mathfrak{z}_j \rangle$ and $\langle \mathfrak{t}_j^\otimes, \mathfrak{r}_i, \mathfrak{z}_i^*, \mathfrak{E}_i, \mathfrak{z}_i^* \rangle$ after querying $\mathcal{C}_1$, where both tuples can pass the validation process. Let $H_2 = H_2(\mathfrak{t}_2^\otimes, \mathfrak{t}_j^\otimes, \mathfrak{E}_j^\otimes \mathcal{G})$ so that $\mathfrak{z}_j = \hat{e}(\mathfrak{t}_j^\otimes H_2 \mathcal{G}, \mathcal{G})$. That is,

$$\begin{aligned} & \prod_{j=1}^n (\hat{e}(\mathfrak{z}_j^* - \mathfrak{z}_j), \mathcal{G}) \\ &= \prod_{j=1}^n \hat{e}(\mathfrak{r}_j \mathfrak{r}_i^\otimes \mathfrak{E}_j^\otimes (H_2^* - H_2) \mathcal{G}, \mathcal{G}). \\ &= \prod_{j=1}^n \hat{e}(\mathfrak{r}_j \mathfrak{E}_j^\otimes (H_2^* - H_2) \mathbb{J}^i, \mathcal{G}) \end{aligned} \quad (10)$$

Hence, assume $\mathbb{J}^i = a\mathcal{G}$ and $\mathfrak{r}_j \mathfrak{E}_j^\otimes = b\mathcal{G}$ for $a, b \in \mathbb{Z}_q^*$ so that $(\mathfrak{z}_j^* - \mathfrak{z}_j) = \mathfrak{r}_j \mathfrak{r}_i^\otimes \mathfrak{E}_j^\otimes (H_2^* - H_2) \mathcal{G} = \mathfrak{r}_j \mathfrak{E}_j^\otimes (H_2^* - H_2) \mathbb{J}^i$. Finally, with $H_2 \neq H_2^*$ and $\mathfrak{z}_i \neq \mathfrak{z}_i^*$, $\mathcal{C}_1$ derives $ab\mathcal{G} = \mathfrak{r}_j \mathfrak{E}_j^\otimes \mathbb{J}^i = (\mathfrak{z}_j^* - \mathfrak{z}_j)(H_2^* - H_2)^{-1}$ and outputs $ab\mathcal{G}$ as the solution to the given CDHP instance, which contradicts with the hardness of the CDHP. $\square$

Theorem 2. *Dynamic identity updating mechanism is provided upon each successful verification so that unlinkability for the specific vehicle is guaranteed.*

Proof of Theorem 2. Assuming the vehicle has passed through $n - 1$ validating sessions by previous RSUs and follows the route $RSU_{n-1} \rightarrow RSU_n$. The current RSU_{n-1} receives $\langle \mathfrak{t}_j^{n-2}, \mathcal{X}_j, \xi_j, \mathfrak{P}_{[j,n-2]}^\prec, Sig_{[j,n-2]}^\otimes \rangle$ from its previous RSU_{n-2} . Upon validation by RSU_{n-1} , $\langle \mathfrak{t}_j^{n-1}, \mathcal{X}_j, \xi_j, \mathfrak{P}_{[j,n-1]}^\prec, Sig_{[j,n-1]}^\otimes \rangle$ is delivered to RSU_n . That is, the vehicle identity has been dynamically updated in different RSU domains as $\{\mathfrak{t}_j^1, \dots, \mathfrak{t}_j^n\}$, where $\mathfrak{t}_j^n = h_2(\mathfrak{t}_j^{n-1}, \mathfrak{r}_j^\otimes \mathcal{G})$.

The relevant signatures are updated in the form of $\mathfrak{P}_{[j,n]}^\prec = \mathfrak{P}_{[j,n-1]}^\prec \mathfrak{P}_{[j,n-1]}^\prec \zeta_j^{h_2(\mathfrak{t}_j^n, \mathfrak{r}_j^\otimes \mathbb{R}^n)}$. $(\mathfrak{r}_j^\otimes)^\mathcal{X}_j \bmod \mathcal{X}_j^2$. Hence, anonymous communication is enabled during all the communication sessions. Notably, each RSU only keeps the two successive vehicle identity as $\mathfrak{t}_j^{n-1} \rightarrow \mathfrak{t}_j^n$, while the historical and future identities are organized by the randomly issued $\mathfrak{r}_j^\otimes \in \mathbb{Z}_q^*$ of each RSU domain. That is, without the assistance of VC, tracing towards an individual vehicle requires the collusion of all the RSUs on the path. Therefore, message linkability for vehicles across various domains can be provided. Moreover, the adopted session key $sk_j = H_4(\mathfrak{t}_j \mathfrak{r}_j \mathcal{G})$ is shared among VC and vehicle, while keeping a secret from each RSU. Overall, impersonate attacks from the compromised RSUs can not be achieved. $\square$

Theorem 3. *The proposed scheme is resistant to replay attack during the entire process. The transmitted messages from past sessions cannot pass the current validation.*

Proof of Theorem 3. During each communication session, data integrity and confidentiality are effectively preserved by the attached timestamps and hashed signatures. Therefore, the delivered packets are mapped to accurate timestamps. Modification or reusing on the previously acquired messages results in failure of the verification process on the receiver side. In device registration, mutual authentication, and cross-domain authentication phases, the fresh timestamps set $\{\mathfrak{t}_1^i, \mathfrak{t}_2^i, \mathfrak{t}_3^i, \mathfrak{t}_4^i, \mathfrak{t}_\infty^i\}$ are used in each communication round. Meanwhile, the signatures involving all transmitted elements are presented. For example, in the mutual authentication phase, the vehicle sends the requesting packet $\langle \text{Request}, \mathfrak{t}_\infty^i, \mathfrak{t}_j^i, \mathfrak{z}_j^i, Sig_V^i \rangle$ to RSU for verification, where the signature $Sig_V^i =$

$h_i(\mathfrak{x}_j || \mathfrak{x}_j || \mathfrak{x}_j || \mathfrak{x}_j) \cdot \mathfrak{r}_j^{\mathcal{G}_i} \bmod \mathcal{G}_i^2$ is calculated with $\langle \mathfrak{x}_j, \mathfrak{x}_j \rangle$. Note that both $\mathfrak{x}_j$ and $\mathfrak{x}_j$ are attached to the current timestamp $\mathfrak{t}_j^i$. Assuming that, in specific duration, $[\mathbb{T}_1, \mathbb{T}_2]$, adversary $\mathcal{A}_1$ has obtained x transmitted requesting packet $\langle \text{Request}, \mathfrak{t}_x^i, \mathfrak{x}_x, \mathfrak{x}_x, \text{Sig}_V^x \rangle_{x \in [1, x]}$ from $\{\mathfrak{x}_1, \dots, \mathfrak{x}_x\}$. $\mathcal{A}_1$ acquires $\mathfrak{t}_A$ and calculates $\text{Sig}_V^A = h_A^{(\mathfrak{x}_A || \mathfrak{x}_A || \mathfrak{x}_A || \mathfrak{x}_A)} \cdot \mathfrak{r}_A^{\mathcal{G}_i} \bmod \mathcal{G}_i^2$. Intuitively, $\forall x \in [1, x]$, and the probability for $\text{Sig}_V^A = \text{Sig}_V^x$ to pass the verification is $\frac{1}{2^d}$, where d denotes the length of Sig_V^A . Hence, our design is resistant to replay attack. $\square$

Theorem 4. *Conditional identity privacy-preserving for both UAVs and RSUs is provided. Anonymity for specific vehicle and UAV is achieved, while the real identity of malicious entities can be revealed if necessary.*

Proof of Theorem 4. As described, the original identity $\mathfrak{x}_T^i \in \{0, 1\}^*$ for validated RSU is kept confidential all the time. Instead, the corresponding session identity is computed as $\mathfrak{x}_T^i = h_1(\mathfrak{t}_1^i, \mathfrak{x}_T^i, \mathfrak{r}_T^i, \mathfrak{s}_T^i)$, which includes the randomly generated $\mathfrak{r}_T^i \in \mathbb{Z}_q^*$ and time-oriented $\mathfrak{t}_1^i$. The RSU session identity varies in each authentication session. Anonymity and message unlinkability in different communication sessions can be provided accordingly. The temporary UAV identity $\mathfrak{x}_j^i = H_2(\mathfrak{x}_U^i, \mathfrak{t}_j^i, \mathfrak{r}_j^i, \mathfrak{g})$ is applied as well, which is only valid within a certain time period and will expire in the future. Note that the distinctive identity $\mathfrak{x}_T^i \in \{0, 1\}^*$ and $\mathfrak{x}_U^i \in \{0, 1\}^*$ remain hidden all the time. Meanwhile, VC stores crucial keying secrets in the remote server. Hence, identity in each session can be further extracted if needed, which offers conditional identity privacy-preserving property for UAVs. As for vehicles, the anonymous identity for initialization is computed as $\mathfrak{x}_j = h_3(\mathfrak{x}_V^i, \mathfrak{r}_j, \mathfrak{g})$. Therefore, vehicle anonymity is provided. With the assistance of RSU edge cluster, VC is able to reveal the original identity according to the stored driving path $RSU_1 \rightarrow RSU_n$. Overall, conditional identity privacy-preserving is enabled in this way. $\square$

5.2. Security Comparison

In this section, the proposed scheme is briefly compared with the existing VANET designs in terms of the crucial security characteristics. The comparison results are shown in Table 2, where the state-of-the-art VANETs authenticated key management schemes PPDAS [19], HABHM [31], and BPAS [32] are discussed. The proposed design is able to meet the desired security requirements.

Table 2. Comparison results on security properties.

Scheme	PPDAS [19]	HABHM [31]	BPAS [32]	The Proposed Scheme
Unforgeability	○	○	○	○
Conditional Anonymity	○	○	×	○
Session Key Establishment	○	○	○	○
Key Escrow Resilience	○	○	○	○
Scalability	×	×	×	○
Efficient Key Updating	○	○	○	○
V2V Connectivity	×	×	×	○
Collusion Attack Resilience	×	○	○	○
Unlinkability	○	○	×	○

6. Performance Analysis

In this section, the performance on the proposed VANET scheme is analyzed. The evaluation on major properties including storage overhead and computation cost is respectively presented for resource-constrained VANETs. The existing schemes PPDAS [19], HABHM [31], and BPAS [32] are evaluated as well.

6.1. Storage Overhead

In the proposed design, the RSU performs as the decentralized edge center for both UAV association and V2V remote data exchange, where the confidential keying information is aggregated and stored. Notably, the design for V2V authenticated key management is discussed in this section in order to compare with other existing schemes, while the storage for UAV association is not included. Meanwhile, the remote VC is able to conduct complicated tasks with sufficient computing ability. Therefore, this section emphasizes RSU storage overhead during the vehicle authentication session. The advantages of our scheme on storage overhead can be illustrated from the comparison results in Figure 3.

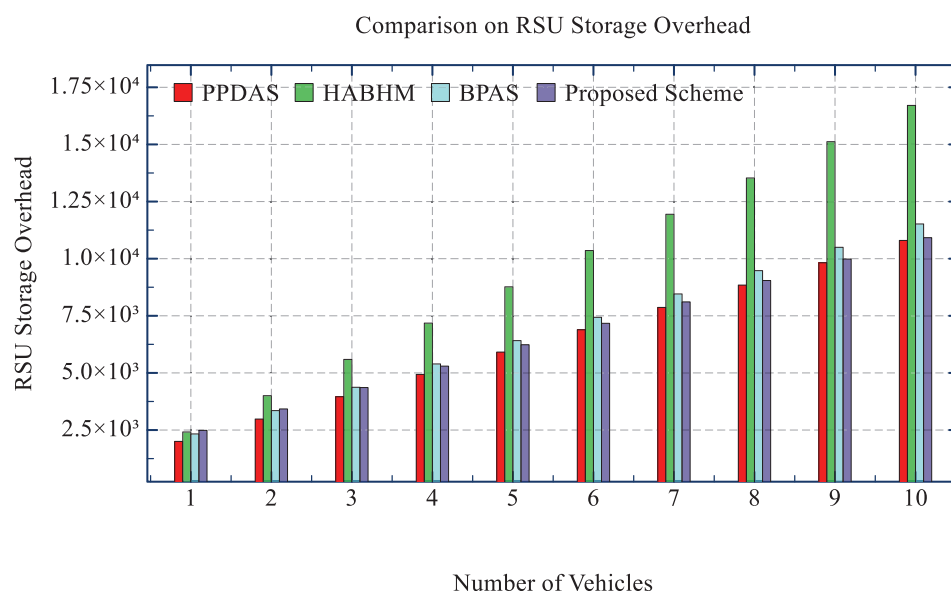


Figure 3. Comparison results on RSU storage overhead.

6.2. Computation Cost

In this section, the computation cost of the proposed design is analyzed. The time consumption for authentication on the RSU side is discussed in terms of the number of participating vehicles. The comparison result with the existing PPDAS [19], HABHM [31], and BPAS [32] are shown in Figure 4. Intuitively, with the batch authentication feature of our scheme, less time consumption is required for the mutual authenticating execution, proving the performance advantages of our design.

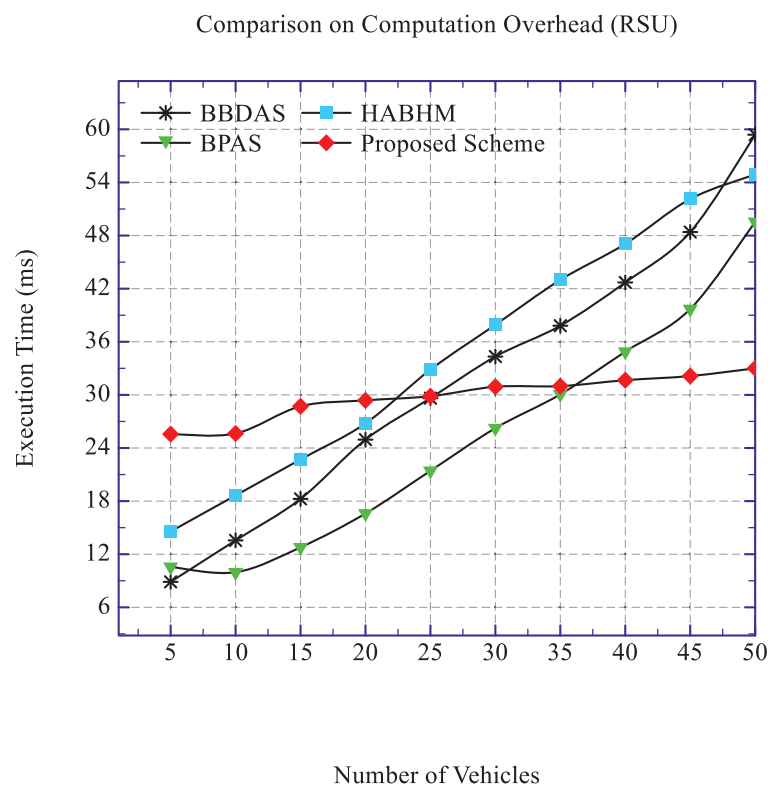


Figure 4. Comparison results on execution time.

7. Conclusions

As the essential functionality of VANET, the spontaneous vehicle-to-vehicle (V2V) message dissemination plays a significant role for instant and real-time data sharing for vehicles within a certain vicinity. Firstly, the remote V2V message delivery intended for long-distance vehicles in the range of different RSUs has not been properly researched. Secondly, both V2V and communication are highly restricted by environmental factors. In this paper, the unmanned aerial vehicles is adopted as the auxiliary facilities for improving the VANET connectivity. The certificateless mutual authentication process for UAV association is developed. The partial secret key is utilized by the central server and UAV itself. Upon verification, the corresponding UAV group key can be generated and safely distributed to the requesting UAVs. The efficient key updating method for all the involved UAVs is achieved. Notably, the dynamic UAV revocation is enabled, while the updated group key is timely acquired by the remaining legitimate UAVs. Meanwhile, the remote V2V message dissemination method is presented, which deploys the decentralized edge RSUs. Particularly, the proposed design is conducted without remote cloud assistance. With the pre-stored driving records collected from the CDA process, the disseminated vehicular message can be forwarded through the edge RSUs and finally transmitted to the destination vehicle. Afterwards, the analysis regarding crucial security properties is presented accordingly, followed by the performance evaluation on storage and time consumption for the authentication process. The comparison results shows that the proposed scheme is able to satisfy the major security and performance requirements. The future works include the further optimization on storage cost and the real VANET implementation of the proposed scheme.

Author Contributions: Conceptualization, H.T.; Methodology, H.T.; Formal analysis, H.T.; Writing—Original Draft Preparation, H.T.; Writing—Review and Editing, H.T.; Supervision, I.C. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by research fund from Chosun University (2020).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lin, C.; Deng, D.; Yao, C. Resource Allocation in Vehicular Cloud Computing Systems With Heterogeneous Vehicles and Roadside Units. *IEEE Internet Things J.* **2018**, *5*, 3692–3700.
2. Hakeem, S.A.A.; El-Gawad, M.A.A.; Kim, H. A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks. *IEEE Access* **2019**, *7*, 119689–119705.
3. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection. *J. Internet Technol.* **2018**, *19*, 481–488.
4. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANETs. *IEEE Trans. Veh. Technol.* **2016**, *65*, 896–911.
5. Lu, R.; Lin, X.; Liang, X.; Shen, X. A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2012**, *13*, 127–139.
6. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746.
7. Cui, J.; Wu, D.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2972–2986.
8. Tan, H.; Chung, I. A Secure Cloud-Assisted Certificateless Group Authentication Scheme for VANETs in Big Data Environment. In Proceedings of the 2019 International Conference on Big Data Engineering (BDE2019), Hong Kong, 11–13 June 2019; pp. 107–113.
9. Lin, X.; Li, X. Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 3339–3348.
10. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1779–1790.
11. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis. *Symmetry* **2018**, *11*, 969.
12. Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *68*, 6709–6717.
13. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network. *IEEE Access* **2019**, *7*, 71424–71435.
14. Shen, J.; Tan, H.; Ren, Y.; Liu, Q.; Wang, B. A Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangement With Adequate Security Assurance. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 31 January–3 February 2016; pp. 693–699.
15. Ma, M.; He, D.; Wang, H.; Kumar, N.; Choo, K.R. An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. *IEEE Internet Things J.* **2019**, *6*, 8065–8075.
16. Tan, H.; Xuan, S.; Chung, I. HCDA: Efficient Pairing-Free Homomorphic Key Management for Dynamic Cross-Domain Authentication in VANETs. *Symmetry* **2020**, *12*, 1003.
17. Wu, L.; Sun, Q.; Wang, X.; Wang, J.; Yu, S.; Zou, Y.; Liu, B.; Zhu, Z. An Efficient Privacy-Preserving Mutual Authentication Scheme for Secure V2V Communication in Vehicular Ad Hoc Network. *IEEE Access* **2019**, *7*, 55050–55063.
18. Wasef, A.; Shen, X. EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Mob. Comput.* **2013**, *12*, 78–89.
19. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749.
20. Zhang, H.; Kumari, S.; Obaidat, M.S.; Wei, F.S. Improving Physical Layer Security via A UAV Friendly Jammer for Unknown Eavesdropper Location. *IET Commun.* **2020**, *14*, 2427–2433.
21. Tan, H.; Chung, I. Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access* **2020**, *8*, 2482–2498.
22. Aliev, H.; Kim, H.; Choi, S. A Scalable and Secure Group Key Management Method for Secure V2V Communication. *Sensors* **2020**, *20*, 6137.
23. Zhou, Y.; Pan, C.; Yeoh, P.L.; Wang, K.; Elakashan, M.; Vucetic, B.; Li, Y. Secure Communications for UAV-Enabled Mobile Edge Computing Systems. *IEEE Transactions on Communications* **2020**, *68*, 376–388.
24. Yoon, K.; Park, D.; Yim, Y.; Kim, K.; Yang, S.K.; Robinson, M. Security Authentication System Using Encrypted Channel on UAV Network. In Proceedings of the 2017 First, IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, 10–12 April 2017; pp. 393–398.
25. Zhou, Y.; Yeoh, P.L.; Chen, H.; Li, Y.; Schober, R.; Zhuo, L.; Vucetic, B. Improving Physical Layer Security via A UAV Friendly Jammer for Unknown Eavesdropper Location. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11280–11284.
26. Tan, H.; Chung, I. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. *IEEE Access* **2019**, *7*, 151459–151474.
27. Lo, N.; Tsai, J. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1319–1328.

-
28. Liu, B.; Jia, D.; Wang, J.; Lu, K.; Wu, L. Cloud-Assisted Safety Message Dissemination in VANET–Cellular Heterogeneous Wireless Network. *IEEE Syst. J.* **2017**, *11*, 128–139.
 29. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. A Scalable Robust Authentication Protocol for Secure Vehicular Communications. *IEEE Trans. Veh. Technol.* **2010**, *59*, 1606–1617.
 30. Pointcheval, D.; Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptol.* **2000**, *13*, 361–396.
 31. Tan, H.; Kim, P.; Chung, I. Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pandemic Control. *Electronics* **2020**, *9*, 1683.
 32. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Trans. Ind. Informatics* **2020**, *16*, 4146–4155.