Secure and Privacy-Aware Incentives-Based Witness Service in Social Internet of Vehicles Clouds

Rasheed Hussain, Donghyun Kim, Junggab Son, Jooyoung Lee, Chaker Abdelaziz Kerrache, Abderrahim Benslimane, and Heekuck Oh

***Abstract*—This paper introduces the concept of a new service for social Internet of Vehicles (IoV)-based clouds called incentives-based vehicle witnesses as a service (IVWaaS), which employs vehicles moving on the road as the witnesses to designated events. Specifically, we focus on two key enablers, a new secure and privacy preserving service framework as well as a new incentive mechanism to promote the wide adoption of the aforementioned social service. In IVWaaS, when confronted any events, the vehicles in the vicinity with mounted cameras collaborate with other roadside cameras to take pictures of the site of interest around them, and send the pictures to the cloud infrastructure anonymously so that the privacy of the vehicles can be preserved. To stimulate active participation from the users, we also introduce a new privacy-aware incentives mechanism called privacy-aware proportionate receipt collection, in which the contributors are credited according to their contribution to the service and can claim their incentives in a privacy-aware fashion. Service providers can also use the stored pictures as "on-demand picture service." Other law enforcement agencies can obtain the stored pictorial information and use it as forensics in the investigations.**

***Index Terms*—Conditional anonymity, incentives, pseudonym exchange, security and privacy, vehicle witnesses, vehicular ad hoc networks (VANETs), vehicular ad hoc networks-based clouds.**

I. Introduction and Related Work

DURING the last couple of decades, vehicular ad hoc networks (VANETs) and Internet of Vehicles (IoV) achieved convincing milestones as a result of which world leading automobile manufacturers started equipping their vehicles with hardware and software to enable smart driving. VANET technology is realized through extensive researches by both academia and industry to let the vehicles talk to each other for safe and infotainment-rich driving experience. To date, there are a number of applications offered by VANET technology ranging from the standard traffic safety applications like cooperative cruise control, emergency warning system, maneuver control, and alleviating highway turbulence to nonsafety infotainment applications such as Internet on wheels, music on the road, video on demand, and real-time traffic information while driving [1], [2]. It is worth noting that communication among vehicles [vehicle-to-vehicle (V2V)] and with the infrastructure [vehicle-to-infrastructure (V2I)] are comparable to the communication in social networks where entities exchange information. Therefore, VANET mimics the social networking-like communication among vehicles and infrastructure as a result of which infotainment, safety, and also social applications and services are realized. It is also worth noting that recently VANET evolved to VANET-based clouds. Abuelela and Olariu [3] proposed a new paradigm shift from VANET to VANET clouds and laid the foundation for VANET clouds. Hussain *et al.* [4] proposed different architectural frameworks for IoV clouds afterward.

Over the last few years, a number of services were proposed for VANET-based clouds (or IoV-based clouds) such as traffic information as a service [5], [6], visual traffic information through clouds [7] and pics-on-wheels (POW) [8]. To the best of our knowledge, Gerla *et al.*'s work, which used vehicles as mobile image collectors and named it POW [8], is the closest to our proposed incentives-based vehicle witnesses as a service (IVWaaS). The witness service is of essence in VANET[1] environment from various perspectives. Such service can be very useful in handling law and order situations (for instance a terrorist attack, a deadly accident, or car lifting etc.), saving forensic evidences for criminal investigation, discouraging benign entities framing, traffic and route management, and fine-grained cooperative awareness etc.

We believe that the success of cloud technology can be leveraged for keeping such service in mind the virtually unlimited resources of the cloud. However, in order to make this service work, the communication between witness and the cloud must be secure to make sure that the contents reach intact at the right destination. Moreover, the contents must also

Manuscript received March 14, 2018; accepted May 29, 2018. Date of publication June 13, 2018; date of current version August 9, 2018. This work was supported by the Institute for Information and Communications Technology Promotion Grant through the Korea Government (A Study on Functional Signature and Its Applications) under Grant 2017-0-01860. *(Corresponding author: Rasheed Hussain.)*

R. Hussain and J. Lee are with the Institute of Information Systems, Innopolis University, Innopolis 420500, Russia (e-mail: r.hussain@innopolis.ru; j.lee@innopolis.ru).

D. Kim and J. Son are with the Department of Computer Science, Kennesaw State University, Marietta, GA 30060 USA (e-mail: donghyun.kim@kennesaw.edu; json@kennesaw.edu).

C. A. Kerrache is with the Department of Mathematics and Computer Science, University of Ghardaia, Ghardaïa 47000, Algeria (e-mail: ch.kerrache@lagh-univ.dz).

A. Benslimane is with the Centre d'Enseignement et de Recherche en Informatique (CERI), University of Avigon, 84911 Avignon, France (e-mail: abderrahim.benslimane@univ-avignon.fr).

H. Oh is with the Department of Computer Science and Engineering, ERICA Campus, Hanyang University, Seoul 426-791, South Korea (e-mail: hkoh@hanyang.ac.kr).

Digital Object Identifier 10.1109/JIOT.2018.2847249

[1]We use the terms "VANET" and "IoV" interchangeably in this paper because both terms exhibit the phenomena where vehicles either communicate with each other or with the infrastructure for information exchange.

be secure during the whole flight. Furthermore, the contents must be safe from the prying eyes of the outsiders/attackers.

The security and privacy are also of paramount importance. The witness should submit the forensics in an anonymous way so that no one, even the law enforcement and insurance agencies, can abuse the witness privacy through tracking. In addition to security and privacy, it is also important that the users must be attracted to use the service. Therefore security, privacy, and motivation for the witness service are essential behind the success of this service and in this paper, we address all three aforementioned problems for the witness service.

Summary of Contributions: This paper is the extension of our previous work [9] and has the following three main contributions.

1) We design the architectural framework for the service keeping in mind its functionality, security, privacy, and incentives. Without loss of generality, we assume that a mechanism already exits to detect the occurrence of the designated events on the road.
2) We propose a novel *identity exchange* mechanism among neighbors to guarantee the conditional anonymity of the contributors. Users carry multiple pseudonyms, and they periodically exchange their pseudonyms among themselves in order to make the communication conditionally anonymous enough so that they cannot be tracked.
3) To stimulate active participation of the contributors on the road, we introduce a new privacy-aware proportionate receipt collection (PPRC)-based incentives mechanism where each vehicle is anonymously credited based on its contribution to the service.

The remainder of this paper is organized as follows. In Section II, we discuss the system models followed by our proposed IVWaaS scheme in Section III. After qualitatively and quantitatively evaluating our proposed scheme in Section IV, we conclude our paper in Section V.

II. System Models

A. System Players and Network Model

The proposed model is the combination of VANET and Cloud Computing. Potential participants of the proposed scheme include mobile sensors (vehicles) fully equipped with VANET DSRC-based on-board unit (OBU), tamper resistant hardware (TRH), cameras, Department of Motor Vehicles (DMV), law enforcing agency(s), revocation authorities (RAs), and judiciary. These are the physical participants of the system. On the other hand, cloud infrastructure is assumed to be in place in order to store and process the pictures (i.e., forensic evidences) and provide them to the judiciary in case of a dispute. Cloud infrastructure consists of software modules/components that include dispatcher, query processor, incentives module, collector, and anonymizer. In order to stimulate active participation of the nodes in IVWaaS service, we included the incentives module in the cloud infrastructure. This module is further divided into one physical entity namely incentives collection point (ICP) which can be a gas station, a mart, and so forth, and four other software submodules, i.e., receipt issuer (RI), receipt receiver, receipt collector (RC), and incentives calculator. The taxonomy of the system participants is shown in Fig. 1.

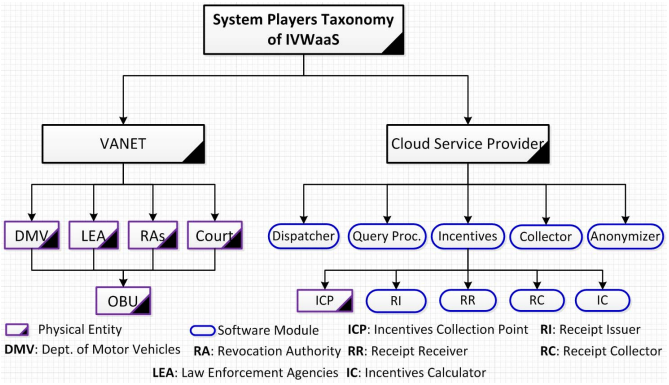

Fig. 1. Taxonomy of the system participants.

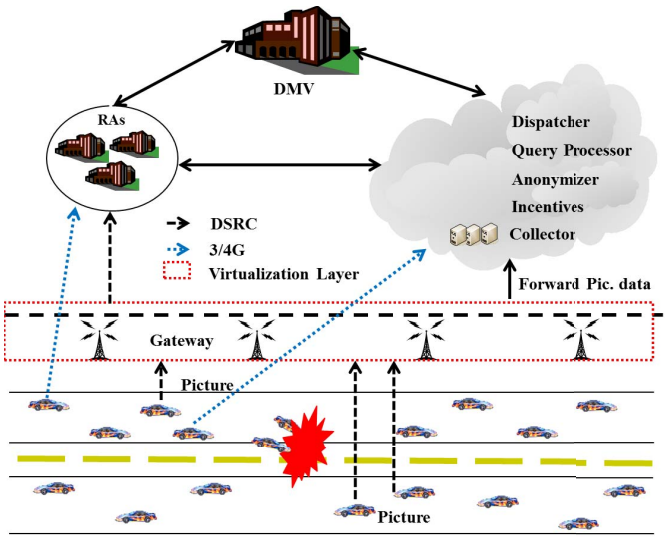

Fig. 2. Proposed network model.

Fig. 2 illustrates the proposed network model. In the proposed network model, vehicles with the help of on-board cameras take pictures of any event and upload it to the cloud either by automatically sensing the situation or by triggering remotely. In this paper, we target the passive service where a set of cameras (both on-board and installed on road if available) are selected to take pictures of the site of interests (SoIs) and send it to the cloud which is then stored as forensic evidences. The best suitable example of passive scenario can be a deadly accident or a terrorist attack.

III. Proposed IVWaaS: Incentives-Based Vehicle Witnesses As Service

A. System Setup

Table I lists all the notations that will be used in the rest of this paper.

1) System Initialization: We use ElGamal encryption algorithm over elliptic curve cryptography to encrypt K_i and K_{V_i}, which will be stored in RAs. Let $\mathbb{G}$ be a cyclic group of prime order q generated by a generator P. DMV randomly chooses $s \in \mathbb{Z}^*$ for its private key and then computes $\text{Pub} = sP$ as its public key. DMV uses threshold-based secret share

TABLE I
NOTATIONS

Notation	Explanation
V_i	*i*-th vehicle/camera of *i*-th vehicle
$\mathbb{G}$	Cyclic group of Order q
P	The generator of $\mathbb{G}$
r	Random nonce
s, s_i	Private master key and *i*-th share of s
Pub	Public key corresponding to s
K^+_{DMV}, K^-_{DMV}	Public private key pair of DMV for signing pseudonyms
K^+_C, K^-_C	Public private key pair of the cloud storage module
u_V	Vehicle V's secret initial counter used in pseudonym generation
o_V	Incrementing factor for pseudonyms
K_i	Vehicle V_i's AES symmetric key used in pseudonym generation
K_{V_i}	V_i's individual secret key
PS^i_V	Vehicle V's ith pseudonym
R_{ID}	Unique receipt/voucher ID
E_{ID}	Event ID
$H(\cdot)$	A MaptoPoint hash function as $H : \{0,1\}^* \rightarrow \mathbb{G}$
$h_k(\cdot)$	Keyed hash function
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation function

scheme [10] and divides s into j parts, where j is the number of RAs. Each RA_i holds one of divided secrets s_i, $1 \leq i \leq j$. In order to construct s from individual s_i, RAs must elect one of them to be a group leader who will be permitted to reconstruct s by receiving more s_is than the threshold and combining them into one.

2) TRH Initialization: In order to install and initialize the black box/TRH in the vehicle, the owner has to personally visit DMV. After confirming the credentials of the vehicle and its owner, DMV initializes TRH and stores the system parameters such as $(\mathbb{G}, q, P, \text{Pub}, u_V, o_V)$ inside the TRH. Additionally, DMV also preloads TRH with vehicle's individual secret key K_{V_i} and pseudonym generation key K_i.

3) Pseudonym Generation: DMV generates pseudonyms for each vehicle at the time of registration. These pseudonyms are stored in the TRH and used for communication in order to preserve the conditional privacy. DMV generates n number of pseudonyms by taking vehicle V's secret counter u_V and increment it by vehicle V's incrementing factor o_V. The pseudonyms are generated as follows:

$$PS^i_V = \{(\alpha)_{K_i} || (\alpha \oplus \text{VID})_{K_{V_i}} || n_i\}_{K^-_{DMV}}$$

where $\alpha = u_V + n_i o_V$, n_i is the current count of generated pseudonym (note that it may not be linear), and VID is the vehicle's ID. Then, DMV stores these pseudonyms in its database and indexes it with the value of n. DMV also saves these pseudonyms along with anonymous certificates in vehicle's TRH and sends the anonymous pseudonyms and certificates to RAs as well. In order to help in revocation, TRH also encrypts K_i and K_{V_i} and sends it to RAs which serves as a trapdoor in revocation. The aforementioned keys are encrypted with public master key using ElGamal encryption as follows:

$$c_1 = rP \text{ and } c_2 = \left(K_i || K_{V_i}\right) \oplus H(rPub)$$

where r is a random nonce selected by the TRH for this encryption, then it sends (c_1, c_2) to RAs. However, RAs can only decrypt the keys K_i and K_{V_i} when they have a warrant to do so and collude to construct s from individual s_i. The reason for saving encrypted keys in RAs' database is twofold: RAs use these keys to revoke a vehicle in case of any dispute and for privacy reasons and we do not want RAs to link pseudonyms and/or extract u_V and o_V from the beacons unless necessary. DMV maintains a database where it saves the credentials of the vehicles (VID, u_V, o_V) whose TRHs are initialized by the DMV. Pseudonyms are maintained by DMV and indexed with the value of n (the counter of pseudonym and to be discussed later) as shown in Fig. 3(a). Moreover, the same kind of table is also maintained by RAs but anonymously as shown in Fig. 3(b).

B. Identity Exchange

Multiple pseudonyms do not help to enhance the user privacy because the pseudonyms can still be traced and linked to the sender [11]. Therefore, we propose a new privacy enhancing mechanism namely *identity exchange* by letting the vehicles in the vicinity exchange pseudonyms. Meanwhile, the privacy is still conditional where the user of the pseudonym is subject to revocation in case it is needed. This way, a node (V_i) can use a pseudonym that it received from node V_j as a result of pseudonym exchange process.

According to DSRC standard, every vehicle in VANET broadcasts its whereabouts information to the neighbors, which includes current location, current speed, heading, and so forth. When a vehicle wants to exchange its pseudonym for privacy preservation, it shows its intention in its beacon messages. We include an *intent* flag in the beacon message that shows the intent of the vehicle for exchanging pseudonyms. The neighbors who receive that beacon have choice if they want to exchange their pseudonyms. The generic beacon denoted by M_b will look like

$$M_b = (B_{\text{data}} || \text{Sec.Primitives} || \text{intent}).$$

B_{data} is the mobility statistics that include current position, speed, acceleration, heading, and other control information such as brake status and steering wheel angle. Sec.Primitives are the parameters that are used for authentication, nonrepudiation, integrity, and so forth. The pseudonym exchange process itself should be anonymous because the knowledge of the pseudonym exchange will give statistical and probabilistic capability to the malicious neighbors and/or attackers to at least know that the exchange took place. To this end, covert communication is the ideal way to carry out pseudonym exchange among the interested set of neighbors. We assume a covert communication-based mechanism which is the variation of a deniable communication mechanism known as DenaLi, to exchange pseudonyms among the neighbors [12]. Inspiring from DenaLi, we use another covert communication-based pseudonym exchange mechanism [13] that leverages regularly broadcasted beacons. Before exchanging pseudonyms, it is important to check the validity of pseudonyms through pseudonym revocation list. The exchange report is sent to RAs anonymously. It is worth noting that if at least one entity of the exchanging entities is benign, then RAs will receive the exchange report.

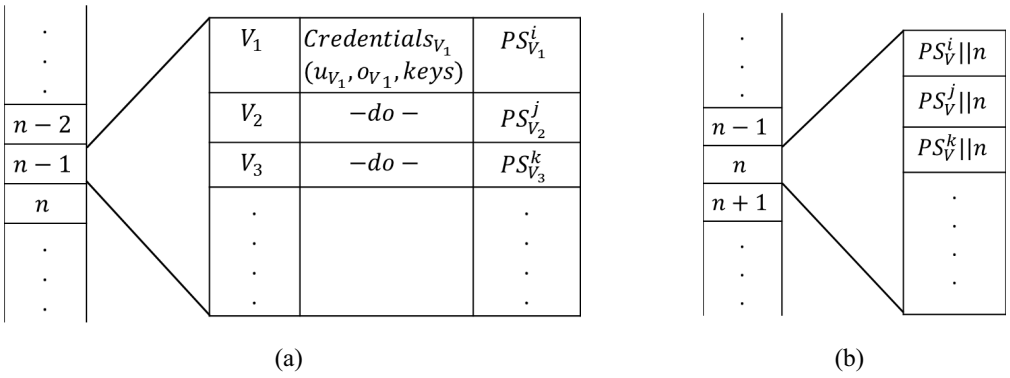

Fig. 3. Pseudonym history tables at (a) DMV and (b) RAs.

Time	Source Pseudonym	Pseudonym Changed For:
t_i	$PS^i_{V_x}$	$PS^j_{V_y}$

Fig. 4. Structure of PEHT.

We note that the revocation privilege has been distributed among a number of RAs rather than a single entity. Therefore, it will be safe to assume that the pseudonym exchange report will reach to any of the available RAs. RAs maintain another database for the exchange history referred to as pseudonym exchange history table (PEHT) which contains time of the exchange, the source pseudonym and the destination pseudonym as shown in Fig. 4.

C. Communication With Cloud

To report an event, each vehicle takes picture of the SoI, and then uploads it to the cloud. The direction of the camera is important for the quality of pictures and for the coverage of SoI. In camera sensor network, such viewing requirement model is known as the full-view model [14]. The operation of these cameras also depend on the density where in case of high vehicular density, designated vehicles must take the pictures whereas in case of sparse density, maximum number of vehicles must take the pictures to cover SoI. To this end, in case of a busy street it is highly possible that there might be more than enough vehicles willing to collaborate. However, it is not desirable for all of them to upload the picture of the SoI since this will incur excessive amount of wireless (Wi-Fi, 3G and/or 4G) traffic. In such a case, only the static cameras around the streets (which are expected to use wired LAN) and the subset of cameras attached to the vehicles should be selected to transmit the pictures of the SoI.

D. Event Reporting and Incentives

In case of pseudonym exchange, we encourage another table namely exchange lock table maintained by RAs in order to prohibit the exchange of the pseudonyms that are used for pictorial events reporting. Individual steps are explained as follows.

1) Reporting Pictorial Event: The vehicle, after taking the picture, the software timestamps it with the GPS information from the GPS module, including one of its pseudonyms from the pool, signs, and sends it to the cloud. The message is constructed in the following way:

$$\text{Vehicle} \rightarrow \text{Cloud:} \quad \left(C_{\text{anony}} \| E_{ID} \| \text{timestamp} \| \text{loc}_V \| \text{loc}_E \| \left(PS^i_V \| Pic\right)_{K_V^-}\right)_{K_C^+}.$$

C_{anony} is the anonymous certificate issued to the vehicle by DMV, E_{ID} is the event ID, loc_V is the location of the vehicle, loc_E is the location where the event happened, PS^i_V is the ith pseudonym of the vehicle and *Pic* is the picture taken.

K_V^- is the private key corresponding to the C_{anony} and K_C^+ is the public key of the cloud module that handles the communication.

2) Receipt/Voucher Collection: After verification of the credentials and the contents provided by the contributor, the RI verifies whether the C_{anony} is valid and not revoked, and also checks validity of the pseudonym. If the credentials are verified, then the cloud provides the vehicle a receipt containing a unique receipt ID that will work as a voucher at the time of redeeming the earned incentives

$$\text{ReceiptIssuer} \rightarrow \text{Vehicle:} \quad \left(C_{\text{anony}} \| \left(E_{ID} \| R_{ID} \| \text{timestamp} \| PS^i_V\right)_{K_C^-}\right)_{K_V^+}.$$

The same information is sent to the RC as well for incentives calculation.

$$\text{ReceiptIssuer} \rightarrow \text{ReceiptCollector:} \quad \left(C_{\text{anony}} \| \left(E_{ID} \| R_{ID} \| \text{timestamp} \| PS^i_V\right)_{K_C^-}\right).$$

All the above values are copied from the original report with an additional unique receipt ID R_{ID}. The receipt ID along with PS^i_V differentiates the report from other reports anonymously in order to claim incentives. The above receipt/voucher is duly signed by the cloud and encrypted with the vehicle's public key, and then it is sent back to the vehicle.

3) Acknowledgment: The vehicle acknowledges the receipt for nonrepudiation. It will not be allowed to redeem the voucher without a valid acknowledgment. This acknowledgment enforces users to use the same pseudonym for the reporting as well as the incentives collection process

$$\text{Ack} : \text{Vehicle} \rightarrow \text{Cloud:} \quad \left(C_{\text{anony}}, \left(R_{ID} \| \text{timestamp} \| PS^i_V \| h_{k_V}(\text{contents})\right)_{K_V^-}\right)_{K_C^+}.$$

In addition to the other values, the vehicle also calculates hash with its individual secret key and includes it in the

acknowledgment, that will be used as a proof in case of any conflict during incentives collection.

4) Redeeming Incentives: In order to redeem earned incentives, the claimer shows all the vouchers to ICP that were collected from the cloud. The cloud receives the following acknowledgment from the vehicle:

$$\text{Ack} : \text{Vehicle} \rightarrow \text{ICP} : C_{\text{anony}} \| E_{ID} \| R_V$$

where R_V is the list of the vouchers earned by vehicle V, such that

$$R_V : \left(E_{ID} \| R_{ID1} \| \text{timestamp} \| PS_V^i\right)_{K_C^-} \left(E_{ID} \| R_{ID2} \| \text{timestamp} \| PS_V^j\right)_{K_C^-}, \ldots \left(E_{ID} \| R_{IDn} \| \text{timestamp} \| PS_V^x\right)_{K_C^-}.$$

After verifying the contents of the vouchers and their validity, ICP verifies the validity of pseudonyms from RAs and also verifies the contribution. RAs send the collective amount of incentives (In_{total}) to the ICP, and ICP provides the vehicle with actual incentives. We assume that the vehicle can provide the ICP with its anonymous bitcoin account and ICP recharges vehicle's account with In_{total} amount of bitcoins. It is also worth mentioning that our scheme is not strictly based on bitcoins but will depend upon the service provider.

5) Contribution Measurement: Incentives are distributed amongst the participating vehicles. One important aspect of the proposed incentives must be fairness. We assume the full-view scheme already in place that gives us the percentage of the full-view from a particular vehicle, denoted by C_j. The contribution of a vehicle is measured based on the output from full-view analysis at that vehicle according to the algorithms outlined in [14]. In addition, we also assume that there is a fixed maximum unit incentive rate, denoted by $X_{\max}$, that is the upper bound for any contributor for a single contribution. The net incentive for jth node, denoted by In_j, is based on the contribution and is given

$$C_j = \text{Full} - \text{View}_j, \text{In}_j = X_{\max} \times \frac{C_j}{100}.$$

The total amount of incentives earned by a vehicle during a time interval Δt is given by: $\text{In}_{j-total} = \sum_i \text{In}_{ji}$.

E. Revocation

To revoke a node, RAs must have obtained a warrant or other authorized letter for the revocation to be carried out. The misbehavior will be assessed by the experts/departments that will include technological experts and/or law enforcement agencies, and decide whether to issue a revocation warrant or not. In order to proceed with revocation, RAs retrieve the forensics from the cloud. The cloud provides RAs with the data related to the time interval provided in the query. After that RAs have to look into the n values of the message to figure out which pseudonym was used. RAs search the pseudonym related to value n and then search the PEHT to figure out whether the pseudonym have been used by its original owner only or exchanged with another user. PEHT will let the RAs know who to follow up. After searching PEHT based on recent time value, RAs collude and construct s from individual s_i related to the pseudonym in question and the session leader decrypts the keys from cipher text $c = \{c_1, c_2\}$ as follows:

$$\begin{aligned} PS_V^i &= c_2 \oplus H(sc_1) \\ &= \left(K_i || K_{V_i}\right) \oplus H(rPub) \oplus H(sc_1) \\ &= \left(K_i || K_{V_i}\right) \oplus H(rPub) \oplus H(srP) \\ &= \left(K_i || K_{V_i}\right) \oplus H(rsP) \oplus H(srP) \\ &= \left(K_i || K_{V_i}\right). \end{aligned}$$

When RAs decrypt the keys K_i and K_{V_i}, RAs decrypts the $(\alpha_i)_{K_i}$ and then extract VID from the pseudonym.

IV. Performance Evaluation

In this section, we quantitatively evaluate our proposed scheme. Our evaluation matrices include security, conditional privacy, and computational and communication overhead incurred by our proposed scheme.

A. Security Analysis

To provide the desired functionality, the proposed IVWaaS must be secure. We assume a passive adversary where he/she can overhear the transmission between the vehicles and cloud service provider. The adversary has an ability of analyzing the overheard data, however, is not able to follow the pseudonym exchange, because the exchange messages are sent anonymous and encrypted. The contents of the picture must be authentic, securely transferred to the cloud and nonrepudiated. Data integrity is guaranteed with the help of hash function; however, we used keyed hash with user individual secret key K_{V_i} to provide data integrity of the report and to provide nonrepudiation because only the sender holds K_{V_i} and nobody else (provided that K_{V_i} is not compromised). Compromise of both keys have critical consequences; however, the compromise of K_i alone will not jeopardize the system because the adversary can obtain only α part of the pseudonym. If both K_i and K_{V_i} are compromised, then the consequences will be catastrophic and the adversary can manipulate pseudonym or reuse it.

Similarly, when a vehicle V reports the event to the cloud, it selects its C_{anony} and a pseudonym PS_V^x, signs the message and then encrypts it with the public key of the cloud. As long as V is not compromised, the communication between cloud infrastructure and the contributors is secure from both outsider and insider adversaries. However, if the public and private key pairs corresponding to C_{anony} are compromised, then the adversaries can use this information to report an event and earn incentives, but the severe consequences like multiple-spending and fraudulence are still mitigated by our proposed scheme.

B. Conditional Privacy

The vehicles anonymously report the events pictorially to the cloud in order to keep the adversaries at bay from singling out the originator of the report. Hence from the reported messages, the privacy of the sender is hard to be abused. With exchanged pseudonyms among nodes, the report is anonymous and cannot be linked to the original owner of the pseudonym. Furthermore, the hashed VID in the pseudonym serves as trapdoor for revocation. To quantify the privacy,

we measure the anonymity of the reporter through entropy denoted by $\mathcal{H}$. For entropy, the anonymity set is the set of the users around the SoI denoted by V and p_{V_i} is the probability that the node V_i is the target witness where $\forall V_i \in V$, $\sum_{i=1}^{|V|} p_{V_i} = 1$. The entropy $\mathcal{H}$ of the target user V_i in the anonymity set V is given by: $\mathcal{H} = -\sum_{i=1}^{|V|} p_{V_i} \times \log_2 p_{V_i}$. Since the anonymity set is V, the possible outcomes can be $|V|$ (with normal distribution) and the probability of each outcome will be $(1/|V|)$. With normal distribution and equally likely involvement of vehicles in exchange of pseudonym in question, the maximum entropy is also given by the following formula: $\mathcal{H}_{\max} = -\sum_{i=1}^{|V|} p_{V_i} \times \log_2 p_{V_i} = \log_2 p_{V_i}$.

It is worth noting that in aforementioned case, the normal entropy is equal to the maximum entropy, i.e., $\mathcal{H} = \mathcal{H}_{\max}$. However, due to the intermittent VANET, such situation is hard to achieve. The entropy of the anonymity does not only depend upon the anonymity set, but also depend upon the individual probability. However in general, the more elements are in anonymity set, the higher entropy is provided that the nodes are distributed equally likely. On the other hand, in our case, the anonymity of the reporter can be variable depending upon its location and traffic density around SoI.

The privacy of the contributor is also preserved in case of incentives because at the time of reporting, the contributor provides the cloud only with a pseudo-identity. This pseudonym may be selected from the contributor's own pseudonym pool or an exchanged pseudonym with a neighbor. Moreover, without compromising the contributor's security parameters, it is hard for adversary to impersonate a benign contributor and to steal the incentives.

Definition 1: Let U be a contributor that receives a receipt R_U from the cloud infrastructure as a result of its contribution. U used a pseudonym $PS_U^i \in \{PS_U^{\{1,\ldots,n\}}\} \vee PS_N^i, N \in \{\text{Neighbor}_U\}$. U presents R_U along with PS_x^i to ICP. Then, redemption is considered to be illegitimate if

$$R_U \in \{\text{Spent List}\} \vee PS_x^i \in \{L_{\text{rev}}\} \vee \Big(PS_x^i \notin \{PEHT\} \wedge PS_x^i \notin \{PS_U^{\{1,\ldots,n\}}\}\Big).$$

Lemma 1: It is hard for adversary to impersonate benign vehicles in our proposed PPRC.

Proof: The vehicle V uploads the picture (taken after an event) to the cloud with anonymous pseudonym PS_V^l (contributor's pseudonym). Anonymous certificate is included in the message and the message is duly signed, i.e., with K_V^- (according to Section III-D). If K_V^- is not compromised, then for any adversary $\mathcal{A}$, it is hard to produce K_V^-', and construct the reporting message signed with K_V^-'. Moreover, C_{anony} corresponding to K_V^-' must also be present for impersonating any other contributor. Under the assumption that DMV uses secure cryptographic mechanism to generate anonymous certificates, it is hard for $\mathcal{A}$ to impersonate any node. When $\mathcal{A}$ constructs the report message with a pseudonym $PS_{\mathcal{A}}^j$, then the RI can easily figure out that pseudonym used to report the event does not correspond to K_V^-' and so does to C_{anony}. The same argument holds for incentives redemption stage as well where the contributor provides ICP with its collected vouchers. The vouchers are duly signed by RI and carry unique R_{ID} and each voucher is bounded with contributor's C_{anony}. If K_V^- is not compromised, then it is hard for $\mathcal{A}$ to impersonate the contributor with fake information. ■

The following corollary follow from the above lemma.

Corollary 1: Providing the same event information multiple times or multiple-spending cannot earn more incentives for a malicious insider adversary $\mathcal{A}_I$.

Let suppose a malicious insider adversary $\mathcal{A}$ presents the list of its collected vouchers $R_V : \{R_{V_1}, R_{V_2}, \ldots, R_{V_k}\}$ at time t_i. ICP checks for the credentials of $\mathcal{A}_I$ and on successful verification and validation, the incentives are credited to $\mathcal{A}_I$. Later on at time t_{i+j}, before the expiry of the redemption period $\Delta t_{E_{ID}}$ of the event E_{ID}, where $[\ldots, t_i, \ldots, t_{i+j}, \ldots] \in \Delta t_{E_{ID}}$, $\mathcal{A}_I$ presents R_{V_2}' to ICP again in order to get more incentives. However, according to above lemma, $\mathcal{A}_I$ cannot forge the voucher because it is signed by the cloud. Redemption at t_i will cause a new entry $(R_{ID2}, PS_{\mathcal{A}_I}^x, \text{timestamp})$ to the *spent list* denoted by L_{spent}. At t_{i+j}, ICP will check the L_{spent} and will find out that $(R_{ID2}, PS_{\mathcal{A}_I}^x, \text{timestamp}) \in L_{\text{spent}}$. Therefore incentives will not be credited to $\mathcal{A}_I$ and hence $\mathcal{A}_I$ is not able to perform multiple spending.

Lemma 2: Redemption process is anonymous in PPRC and it does not reveal the real identity of the claimer.

Proof: In PPRC, at the redemption stage, the vehicle provides the ICP with $(\{C_{\text{anony}}\} \| \{E_{ID}\} \| R_V)$, where $\{C_{\text{anony}}\}$ is the list of anonymous certificates used for different reports and different events, and R_V is the list of the vouchers for redemption. The ICP extracts each voucher from the list and validates its contents. The most valuable information that ICP can get is the pseudonym PS_V^x which is $\{(\alpha)_{K_x} \| (\alpha \oplus \text{VID})_{K_{V_x}} \| n_x\}_{K_{DMV}^-}$. Without the information about K_{V_x} and K_x, ICP cannot know the VID that is encapsulated in the pseudonym. the ICP can check for the revocation status of the pseudonym and its authenticity by verifying the signed pseudonym. Moreover, the ICP cannot link any pseudonym to an individual user because the pseudonym may have been exchanged with somebody else in that case PEHT should be processed to figure out the exchange history. ■

C. Computation and Communication Overhead

On the basis of the underlying assumption that a portion of vehicular density on the road and particularly in SoI, have 4G data plans, the communication overhead might not phenomenally degrade the service because the overhead is divided into different frequencies of DSRC and 4G. Nevertheless, the number of nodes at SoI that have 4G connection and DSRC-based OBU may affect the overall quality of services. Hence, a normal distribution of both aforementioned standards would produce better results.

To report an event, an OBU performs $1E + 1H$, where E denotes the asymmetric encryption of the whole message, and H denotes the hash calculation of the contents. Revocation cost is divided into two scenarios, direct and indirect revocation. In case of direct revocation, the cost denoted by $T_{\text{dir-rev}}$ is given by

$$T_{\text{dir-rev}} = \text{Cost}\big(\text{SearchTable}_{\text{pseu}} \& PEHT\big) + \text{Cost}\big(\text{Extract } K_i, K_{V_i}\big) + \text{Cost}(\text{Symm.Decryption})$$
$$T_{\text{dir-rev}} = 2T_\lambda + 2T_{\text{mul}} + 2T_H + 2T_{\text{sym-dec}}.$$

TABLE II
COMPARISON WITH KNOWN INCENTIVES SCHEMES

Scheme	Redemption Cost	Privacy	Tracing & Profilation at redemption	ID Disclosure	ID Linkage	Incentives selling & purchase
Park et al. [18] and Lee et al. [19]	$2j \times (Verify_{Sig})$ $+x \times (Verify_{Sig})$	✗	✓	✓	✓	✗
Li et al. [20]	$2n \times (Verify_{Sig})$	✗	✓	✓	✓	✗
Tseng et al. [21]	$Verify_{Sig} + 2List - Search$ $+$*Convex vector comb.*	✗	✓	✓	✓	✗
Q.Li et al. [17]	$(C_{max} + 2) \times Verify_{Sig}$	△	✓	✓	✓	✗
Our Scheme	$0.78j + j \times Verify_{Sig}$	✓	✗	✗	✗	✓

T_λ is the time incurred by the table search ($\text{Table}_{\text{pseu}}$-pseudonym table and PEHT), T_{mul} is the time required for point multiplication, T_H is the time required to calculate hash, and $T_{\text{sym}-\text{dec}}$ is the time required for symmetric decryption. For indirect revocation, RA examines all nodes that use current pseudonym in question (used simultaneously). Hence, the revocation consists of two steps: 1) pin point the nodes that possessed and 2) used the pseudonym and compare their $h_{K_{V_i}}(\cdot)$ value with the pseudonym in question. The revocation cost of the indirect revocation denoted by $T_{\text{indir}-\text{rev}}$ is given by:

$$T_{\text{indir}-\text{rev}} = 2T_\lambda + 2\sum_{i=1}^{j}\left(T_{mul_i} + T_{H_i} + T_{\text{sym-dec}_i}\right) + \sum_{i=1}^{j} T_{h_{i,k}}.$$

$T_{h_{i,k}}$ is the time required for keyed hash calculation and in case of indirect revocation, RAs have to examine j number of nodes. In [10], T_{mul} is found for a supersingular curve with embedding $k = 6$ over $\mathbb{F}_{3^{97}}$ to be equal to 0.78 ms. Hence, the above equations can be written as

$$T_{\text{dir}-\text{rev}} = 1.56 + 2\left(T_\lambda + T_H + T_{\text{sym}-\text{dec}}\right)$$

$$T_{\text{indir}-\text{rev}} = 2T_\lambda + j \times 1.56\sum_{i=1}^{j}\left(T_{H_i} + T_{\text{sym-dec}_i}\right) + \sum_{i=1}^{j} T_{h_{i,k}}.$$

In case of incentives redemption, there are three major functions, two of which are carried out by the ICP and the other is carried out by the vehicle. In the incentives redemption stage, the cost is denoted by T_{redemp} and is given by

$$\begin{aligned} T_{\text{redemp}} &= j \times \left(\text{Cost}\left(\text{Verify}_{\text{Sig}}\right) + \text{Cost(3SearchTable)}\right. \\ &= j \times \left(2T_p + T_{\text{mul}} + 3T_\lambda\right) \\ &= 0.78j + j \times \left(2T_p + 3T_\lambda\right) \text{ ms.} \end{aligned}$$

j is the number of vouchers, $\text{Verify}_{\text{Sig}}$ is the signature verification function whose cost is equal to $(2T_p + T_{\text{mul}})$ [15]. T_p is the time required to perform pairing operation, and there are three table searches involved in case of incentives redemption. The ICP searches for the revocation status of the pseudonym, exchange status of the pseudonym, and redemption status of the vouchers in the respective tables.

The communication overhead incurred by our proposed scheme is partially fixed. In case of pictorial reporting message or contribution, communication overheard is $197 + \beta$, where β is equal to $\text{Contents} + \text{Size}_{\text{Pseudonym}}$. The certificate size according to our assumption [15] is 125 *bytes*, and the signature is 56 *bytes* long. We use Harri *et al.*'s [16] implementation, where timestamp and *location* are 2 *bytes* and 6 *bytes*, respectively. The overhead incurred by the communication from vehicle to cloud (while reporting event) is equal to $197 = 125+56+2+2+6+6$. Similarly at the redemption stage, the communication overhead becomes $62j + j \times PS_V^x$, where each voucher size is $2+2+2+56+PS_V^x = 62+PS_V^x$ and j is the number of vouchers that the contributor wants to redeem.

For full view of SoI, the road topology is different from the sensor networks and is firmly fixed, but due to the possibility of fixed roadside cameras, according to full-view algorithm [14], the total running time is polynomial function of the total number of vehicles. Full view method requires $O((k+l)^2)$ where $(k+l) \leq V$, k is the number of vehicles in SoI is and l is the number of fixed roadside cameras.

D. Comparison With Known Incentives Schemes

From Table II, it can be seen that our scheme offers more incentives functionalities than the previous schemes. Although our scheme and previous schemes are not directly comparable; however, one of the huge difference is that we guarantee full conditional privacy right from the reporting all the way till redemption of the incentives. According to Table II, previous schemes do not consider privacy except Li and Cao [17]. However, Li and Cao scheme, the real identity must be revealed at the redemption stage. That is why the privacy is not preserved properly. The anonymous incentives redemption adds robustness to our system where any contributor can sell or purchase its vouchers to earn revenue as well whereas other proposed schemes do not have this feature. Our proposed scheme also outperforms other schemes from incentives redemption standpoint.

V. CONCLUSION

In this paper, we proposed a secure and privacy-aware witness service for social VANET-based clouds. Vehicles along with the fixed cameras on the road, take the picture of the incident on the road and upload it to the cloud in secure and privacy-preserving way. Cloud on the other hand, stores the pictorial information for long-term use such as, on-demand pictorial service, providing forensic evidences to law enforcement agencies and insurance agencies. We introduced a new

secure and privacy-aware witness service on the move through the identity-exchange-based privacy preservation mechanism. To stimulate active participation from the neighbors, we introduced the PPRC mechanism where each contributor is credited with incentives according to their contribution. In our proposed scheme, the privacy is preserved throughout the service right from event reporting to the incentives redemption.

REFERENCES

[1] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VANET-based secure taxi service," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2381–2390, 2013.

[2] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[3] M. Abuelela and S. Olariu, "Taking VANET to the clouds," in *Proc. ACM 8th Int. Conf. Adv. Mobile Comput. Multimedia*, Paris, France, 2010, pp. 6–13.

[4] R. Hussain, Z. Rezaeifar, and H. Oh, "A paradigm shift from vehicular ad hoc networks to VANET-based clouds," *Wireless Pers. Commun.*, vol. 83, no. 2, pp. 1131–1158, 2015.

[5] R. Hussain, F. Abbas, J. Son, and H. Oh, "TIaaS: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks," in *Proc. IEEE Int. Symp. Cluster Comput. Grid*, Delft, The Netherlands, 2013, pp. 178–179.

[6] R. Hussain, Z. Rezaeifar, Y.-H. Lee, and H. Oh, "Secure and privacy-aware traffic information as a service in VANET-based clouds," *Pervasive Mobile Comput.*, vol. 24, pp. 194–209, Dec. 2015.

[7] D. Kwak, R. Liu, D. Kim, B. Nath, and L. Iftode, "Seeing is believing: Sharing real-time visual traffic information via vehicular clouds," *IEEE Access*, vol. 4, pp. 3617–3631, 2016.

[8] M. Gerla, J.-T. Weng, and G. Pau, "Pics-on-wheels: Photo surveillance in the vehicular cloud," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, San Diego, CA, USA, 2013, pp. 1123–1127.

[9] R. Hussain *et al.*, "Vehicle witnesses as a service: Leveraging vehicles as witnesses on the road in VANET clouds," in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, vol. 1. Bristol, U.K., Dec. 2013, pp. 439–444.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Phoenix, AZ, USA, 2008, pp. 246–250.

[11] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proc. IEEE 7th Int. Conf. Wireless Demand Netw. Syst. Services (WONS)*, 2010, pp. 176–183.

[12] A. Narain, N. Feamster, and A. C. Snoeren, "Deniable liaisons," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Scottsdale, AZ, USA, 2014, pp. 525–536.

[13] R. Hussain, D. Kim, A. O. Tokuta, H. M. Melikyan, and H. Oh, "Covert communication based privacy preservation in mobile vehicular networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Tampa, FL, USA, 2015, pp. 55–60.

[14] Y. Wang and G. Cao, "On full-view coverage in camera sensor networks," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 1781–1789.

[15] K.-A. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5386–5393, Nov. 2013.

[16] J. Harri, F. Filali, and C. Bonnet, "Rethinking the overhead of geo-localization information for vehicular communications," in *Proc. IEEE 66th Veh. Technol. Conf. (VTC Fall)*, Sep. 2007, pp. 2111–2115.

[17] Q. Li and G. Cao, "Providing privacy-aware incentives for mobile sensing," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, San Diego, CA, USA, Mar. 2013, pp. 76–84.

[18] J.-S. Park and S. Beak, "Securing one-way hash chain based incentive mechanism for vehicular ad hoc networks," *Peer Peer Netw. Appl.*, vol. 7, no. 4, pp. 1–6, 2012.

[19] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2715–2728, Jul. 2012.

[20] F. Li and J. Wu, "FRAME: An innovative incentive scheme in vehicular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dresden, Germany, Jun. 2009, pp. 1–6.

[21] F.-K. Tseng, Y.-H. Liu, J.-S. Hwu, and R.-J. Chen, "A secure reed–solomon code incentive scheme for commercial ad dissemination over VANETS," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4598–4608, Nov. 2011.

Rasheed Hussain is currently an Assistant Professor with Innopolis University, Innopolis, Russia. He was also a Guest Researcher with the University of Amsterdam, Amsterdam, The Netherlands, from 2015 to 2016. His current research interests include information security and privacy, applied cryptography, vehicular ad hoc networks (VANET), vehicular social networks, VANET-based clouds, blockchain, Internet of Things, and named data networking.

Donghyun Kim is an Associate Professor with the Department of Computer Science, Kennesaw State University, Marietta, GA, USA. From 2010 to 2016, he was an Assistant Professor with the Department of Mathematics and Physics, North Carolina Central University, Durham, NC, USA. His current research interests include security and privacy, social computing, mobile computing, cyber physical systems, wireless and sensor networking, and algorithm design and analysis.

Junggab Son received the Ph.D. degree from ERICA Campus, Hanyang University, Ansan, South Korea.

He is currently an Assistant Professor with the Department of Computer Science, Kennesaw State University, Marietta, GA, USA. His current research interests include applied cryptography, security and privacy issues on significant applications, which includes cloud computing (Fog/Edge computing), Internet of Things (Future Internet), vehicular ad hoc network, social network services, and bioinformatics.

Jooyoung Lee is currently an Assistant Professor with Innopolis University, Innopolis, Russia. Her current research interests include social network analysis, reputation managements, algorithmic graph theory, and game theory.

Chaker Abdelaziz Kerrache is an Assistant Professor with the Department of Maths and Computer Science, University of Ghardaia, Ghardaïa, Algeria. His current research interests include trust and risk management, secure multihop communications, vehicular networks, named data networking, and UAVs.

Abderrahim Benslimane has been a Professor of computer science with Avignon University, Avignon, France, since 2001. He was a Technical International Expert with the French Ministry of Foreign and European Affairs from 2012 to 2016. He has been an Associate Professor with the University of Technology of Belfort-Montbéliard, Belfort, France, since 1994. He has authored or co-authored over 150 refereed international publications.

Prof. Benslimane is the Editor-in-Chief of *Multimedia Intelligence and Security Journal*, an Area editor of Wiley's *Security and Privacy Journal*, and an editorial member of *IEEE Wireless Communication Magazine* and Elsevier's *Ad Hoc Networks*. He has been serving as the General-Chair of IEEE WiMob since 2008. He lunched and has been serving as the General-Chair of MoWNet since 2011. He served as the Symposium Co-Chair/Leader in many IEEE international conferences, such as ICC, Globecom, AINA, and VTC. He is the Chair of the IEEE Communication Society TC of Communication and Information Security.

Heekuck Oh received the B.S. degree in electronics engineering from Hanyang University, Seoul, South Korea, in 1983. and the M.S. and Ph.D. degrees in computer science from Iowa State University, Ames, IA, USA, in 1989 and 1992, respectively.

He is currently a Professor with the ERICA Campus, Hanyang University. His current research interests include network security and cryptography.

Prof. Oh is the President of the Korea Institute of Information Security and Cryptology and a member of the Advisory Committee for Digital Investigation in Supreme Prosecutors' Office, South Korea. He is also a member of the Advisory Committee for Internet Security under the Korea Communications Commission.