Vehicle Witnesses as a Service: Leveraging Vehicles as Witnesses on the Road in VANET Clouds

Rasheed Hussain*, Fizza Abbas*, Junggab Son*, Donghyun Kim†, Sangjin Kim‡, and Heekuck Oh*
* Department of Computer Science and Engineering, Hanyang University, ERICA Campus, South Korea
E-mail: {rasheed, hkok}@hanyang.ac.kr
† Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA
E-mail: donghyun.kim@nccu.edu
‡ Department of Computer Science and Engineering, Korea University of Technology and Education
E-mail: sangjin@koreatech.ac.kr

Abstract—Inspired by the dramatic evolution of VANET-clouds, this paper proposes a new VANET-cloud service called VWaaS (Vehicle Witnesses as a Service) in which vehicles moving on the road serve as anonymous witnesses of designated events such as a terrorist attack or a deadly accident. When confronted the events, a group of vehicles with mounted cameras collaborate with roadside stationary cameras to take pictures of the site of interest (SoI) around them, and send the pictures to the cloud infrastructure anonymously. The pictures are sent to the cloud in a way that the privacy of the senders can be protected, and kept by the cloud for future investigation. However, for the case that the pictures are used as an evidence of court trial, we made the privacy protection to be conditional and thus can be revoked by authorized entity(s) if necessary.

Keywords—VANET, VANET-clouds, Vehicle Witnesses, Security and Privacy, Conditional Anonymity, Pseudonym Exchange.

I. INTRODUCTION

Today’s high-end cars are not the same century-old boxes with four wheels anymore, but rather more complex and sophisticated machines that are dreamed to bring reliability and safety to our driving experience. The latter is being realized through extensive researches conducted by both industry and academia, collectively referred to as Vehicular Ad hoc NETwork (VANET). Recently, world leading car manufacturers such as BMW, Audi, Toyota, and Ford, to name a few, have begun outfitting their cars with such technology. Nevertheless, security and privacy issues are still hot topics in VANET [1], [2]. Besides, VANET is rapidly evolving to VANET clouds as a result of the new resource-rich high-end cars. Oiarzu et al. envisioned a new paradigm shift from traditional VANET to autonomous VANET clouds [3], and Hussain et al. later on proposed different architectural frameworks for VANET-based clouds [4]. Recently, a number of services were proposed for VANET-based clouds. TlaaS (Traffic Information as a Service) [5], and POW (Pics-On-Wheels) [6] are two of them.

To the best of our knowledge, POW is the first approach to use vehicles to collect lively images of an area specified by a query from a user. Once the query is broadcasted, each vehicle nearby the scene will take a picture of its surroundings using an onboard camera and send it back to the user. They also discuss about street surveillance which can be very useful to save evidences for future investigation and insurance claims. With this mobile surveillance system, the law enforcement agencies can timely confirm an accident and get mobilized. Furthermore, the system will discourage the forgery of forensic evidences since any vehicle nearby the scene could have sent an original forensic evidence to the cloud. Unfortunately, Gerla et al. [6] did not provide any detail of such surveillance system, e.g. underlying architecture, despite the fact that this kind of VANET based surveillance system is much more demanding than the on demand basis simple image collecting system proposed by them. To fill this deficiency, this paper investigates a road surveillance system using VANET clouds.

Contributions. This paper introduces a new service mechanism atop the VANET-clouds infrastructure called VWaaS (Vehicle Witnesses as a Service). The proposed service utilizes the mounted cameras on the cars along with fixed roadside cameras to provide pictorial services to other entities (for instance VANET users and/or law enforcement agencies). Once a designated event occurs, the vehicular nodes serve as witnesses to the event and provide the forensic evidences to the law enforcement agencies for investigation. Note that we assume the existence of a mechanism for the VANET to detect the occurrence of a designated event since it is out of the scope of this paper. Our systems is carefully designed in terms of security and privacy. This includes a conditional privacy mechanism for the identity of the vehicles by allowing them to regularly exchange their pseudonyms, which is revocable if requested by a legitimate legal authority.

The remainder of the paper is organized as follows. Section II outlines the state of the art regarding privacy issues in VANET and VANET clouds. In Section III, we discuss the system and network model followed by our proposed scheme in Section IV. After evaluating our proposed scheme in Section V, we conclude our paper along with the future directions in Section VI.

II. STATE OF THE ART

In the following subsections, we present a survey on security and privacy issues in VANET and a survey on VANET-cloud services.

A. Security and Privacy in VANET

Security and privacy issues have been long chased in VANET. Here, we particularly outline the state of the art regarding privacy issues in VANET. In order to preserve privacy, the multiple pseudonymous strategy is regarded as
one of the best solutions so far in VANET. As a result, several schemes have been proposed that exploit multiple pseudonyms. 

In [7], authors put multiple pseudonyms into practice in order to preserve privacy whereas Ma et al. [8] discussed the refilling strategy for multiple pseudonyms-based schemes. Beresford et al. [9] proposed the concept of Mix Zone which is used as a hotspot for changing pseudonyms in order to provide unlinkability among pseudonyms that are sent by the same vehicle. Whenever a vehicle traverses through such a zone, it will have a chance to change its current pseudonym. A different approach was taken by Hussain et al. [10] to conditionally preserve privacy in VANET by proposing identityless beaconing mechanism. In their scheme, the vehicles broadcast beacon messages anonymously without any identity information.

Unfortunately, changing pseudonyms does not necessarily preserve privacy. Wiedersheim et al. figured out that even if a unique pseudonym is used with each message, movement profiles could still be generated and the vehicles could be traced [11]. This led Eckhoff et al. [12] to propose an identity diffusion scheme where users swap their identities with neighbors using predefined time slots. However, the time-dependent pseudonym swapping can still have an adverse effect on the privacy because the pseudonyms are bounded by the time window and the degree of anonymity depends upon the length of the time window. Therefore, to provide conditional privacy and anonymous communication, this paper proposes a new flexible identity-exchange mechanism, where the neighbors exchange identities with each other, but the revocation authorities can still trace back to the vehicle, if needed. One important requirement is that a vehicle must not be able to frame other benign nodes.

B. VANET-based Cloud Services

VANET-based cloud is still an infant among the research community yet. Some of the researchers have taken initiative to propose different services that this field can offer. Olariu et al. took the credit to initiate this paradigm shift from VANET to VANET-based clouds by taking VANET to the clouds [3]. Hussain et al. [4] proposed different architectural frameworks for vehicular clouds. Recently, Hussain et al. [5] proposed a traffic information dissemination scheme namely TaaS (Traffic Information as a Service) in VANET clouds where vehicles cooperate with clouds in the form of mobility data and cloud intelligently provides the vehicles with the traffic information based on their current and near-future locations. Gerla et al. [6] proposed a mobile cloud-based scheme called POW (Pics-on-Wheels) that delivers pictures on demand, to the citizens by using vehicles cameras. In their scheme, anybody can query the cloud to provide that entity with the picture of a ZoI (Zone of Interest). Cloud infrastructure designates users near ZoI to take pictures on the requester’s behalf. However, they do not address any security and privacy issues. Because without security and privacy measures, such service may have catastrophic consequences such as privacy abuse, framing, and content and/or forensic manipulation. We on the other hand, address aforementioned concerns and propose a full picture of the pictorial service used for variety of purposes in VANET-based Clouds.

III. SYSTEM AND NETWORK MODEL

A. System Participants

The proposed model is the combination of VANET and Cloud Computing. Potential participants of the proposed scheme include mobile sensors (vehicles) fully equipped with DSRC-based On-board Unit (OBU), TRH (Tamper Resistant Hardware), cameras, Department of Motor Vehicles (DMV), law enforcing agency(s), Revocation Authorities (RAs), and judiciary. 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.

B. Network Model

The proposed network model is shown in figure 1. Figure 1 illustrates the proposed network model. In the proposed network model, vehicles with the help of on-board cameras take the pictures of any event and upload it to the cloud. It is worth noting that the picture taking services can be either active or passive. Active service refers to a scenario where participating vehicles take pictures of the vicinity after specified time interval and then upload the pictures to the cloud. Whereas in Passive service, vehicles proactively take pictures as a result of certain events or unless they are directed to do so. 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 the pictures of Sol (Site of Interest) and send it to the cloud where it is saved as forensic for future investigation.

C. Baseline

For better understanding of the proposed scheme, we take a special use-case of the passive picture taking service where vehicles, after getting instructions from the cloud or by detecting any event, take pictures of the scene and send it over to cloud. For instance, in case of a deadly accident on the road, in order to save the true forensics of the incident, vehicles in the vicinity take pictures of Sol. However to remedy any
abuse against user or its location privacy, we leverage multiple pseudonyms in vehicles where they can exchange pseudonyms with their neighbors. Such exchange of pseudonym increases the anonymity of vehicles but at the same time poses severe threats, for instance framing benign vehicles and so forth. Hence we use an efficient tracing mechanism for that purpose. Even if the vehicle is using anybody else’s pseudonym, it is subject to revocation in case of any dispute.

IV. PROPOSED VEHICLE WITNESSES AS A SERVICE

In this section we outline our proposed secure and privacy-aware surveillance system referred to as VWaaS. In the proposed scheme, vehicles after either discovering an event (for instance black ice on the road or a traffic jam), or after getting directives from cloud infrastructure, take pictures of the SoI (Site of Interest) and send it to the cloud. Cloud on getting directives from cloud infrastructure, take pictures of the back of the head of a person is not useful if the object is taken from a very specific angle. For instance, black ice on the road or a traffic jam), or after discovering an event (for instance black ice on the road or a traffic jam). For instance, black ice on the road or a traffic jam), or after discovering an event.

1) System Initialization: We use ElGamal encryption algorithm [13] over the ECC (Elliptic Curve Cryptography) [14] to encrypt $K_j$ and $K_{VL}$, and save them into RAs. Let $G$ be a cyclic group of prime order $q$ where $G$ is generated by $P$. DMV first chooses $s \in \mathbb{Z}^*$ as its private key and computes $Pub = sP$ as its public key. DMV then uses threshold based secret share scheme [15] and divides $s$ into $j$ parts where $j$ is the number of RAs. Each $RA_i$ holds a share $s_i$, and $s = (s_1, s_2, s_3, ..., s_j)$. In order to construct $s$ from individual $s_i$, RAs must elect one of them to be group leader and construct $s$ from combination of $s_i$.

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 saves the system parameters in the TRH including $(G, q, P, Pub, u_{V}, o_{V})$. Additionally DMV also preloads TRH with vehicles individual secret key $K_V$ and pseudonym generation key $K_i$.

3) Pseudonym Generation: 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: $PS^V = \{(\alpha)_{K_V}||{(\alpha \oplus VID)_{K_{VL}}}||n_i\}_{K_{DMV}}$ 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 vehicular ID. Then DMV stores these pseudonyms in its database and indexes it with the value of $n$. After all pseudonyms are generated for the vehicle, DMV saves these pseudonyms in vehicles TRH and sends the anonymous pseudonyms to RAs as well. In order to help in revocation, TRH also encrypts $K_i$ and $K_{VL}$, 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: $c_1 = r P$, $c_2 = (K_i)_{K_{VL}} \oplus H(rPub)$. 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 $K_{VL}$ 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; we do not want RAs to link pseudonyms and/or extract $u_{V}$ and $o_{V}$ from the beacons until necessary otherwise. DMV maintains a database against each vehicle whose TRH is initialized by DMV and saves the credentials of each vehicle $(VID, u_V, o_V)$. 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. 2(a). Moreover the same kind of table is also maintained by RAs but anonymously as shown in Fig. 2(b). In other words, the pseudonyms do not carry any information that would enable RAs to link them to the owner.

B. Communication with the Cloud

To provide the anonymous witness services, VANET users first subscribe for the service with the cloud showing their interest. In order to report an event to the cloud, each vehicle (more precisely its OBU) activates the picture-taking function, takes a series of pictures at once, and then uploads them to the cloud. A picture of an object is useful only if the picture of the object is taken from a very specific angle. For instance, a picture of the back of the head of a person is not useful

<table>
<thead>
<tr>
<th>Notation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_i$</td>
<td>$i$-th vehicle/camera of $i$-th vehicle</td>
</tr>
<tr>
<td>$G$</td>
<td>Cyclic group of Order $q$</td>
</tr>
<tr>
<td>$P$</td>
<td>The generator of $G$</td>
</tr>
<tr>
<td>$r$</td>
<td>Random nonce</td>
</tr>
<tr>
<td>$s_i$</td>
<td>Private master key and $i$-th share of $s$</td>
</tr>
<tr>
<td>$Pub$</td>
<td>Public key corresponding to $s$</td>
</tr>
<tr>
<td>$K_{DMV}$</td>
<td>Public private key pair of DMV for signing pseudonyms</td>
</tr>
<tr>
<td>$K_{VL}$</td>
<td>Public private key pair of the cloud storage module</td>
</tr>
<tr>
<td>$V_{sP}$</td>
<td>Vehicle $V$’s secret initial counter used in pseudonym generation</td>
</tr>
<tr>
<td>$u_{V}$</td>
<td>$V$’s AES symmetric key used in pseudonym generation</td>
</tr>
<tr>
<td>$K_{VL}$</td>
<td>$V$’s individual secret key</td>
</tr>
<tr>
<td>$PS^V$</td>
<td>$V$’s pseudonym</td>
</tr>
<tr>
<td>$H(\cdot)$</td>
<td>A MapToPoint hash function as $H: {0,1}^* \rightarrow G$</td>
</tr>
<tr>
<td>$h_{ub}(\cdot)$</td>
<td>Keyed hash function</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>Exclusive OR operation</td>
</tr>
<tr>
<td>$</td>
<td></td>
</tr>
</tbody>
</table>

TABLE I: Notations
to identify the person. Due to the aforementioned reason, to obtain a vivid description of SoI, it will be desirable to obtain the visual information from every direction if possible. In the area of camera sensor network, such as visual requirement model is known as the full-view model [16]. In case of a less busy street, we may not have enough vehicles in the vicinity which have subscribed for the service. Therefore, all vehicles in the area will be needed to upload the images of the scene to best support the full-view image construction of the SoI. On the other hand, in case of a busy street, it is highly possible that there might be more vehicles than enough nearby 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 (Wifi, 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.

In [16], the authors discuss about the necessary and sufficient conditions to check if an area is full-view covered by a group of homogenous (i.e. equal hardware capability) camera sensors. However, the camera sensors that we are considering in this paper are more likely to be heterogeneous. The sufficient and necessary conditions to check if an area is full-view covered by a group of heterogeneous camera sensors by Wu and Wang [17] is more applicable to our situation. One way to elect a smaller subset of cameras to obtain the full-view image of the SOI while minimizing the wireless traffics from the vehicles would be (a) allowing all the static cameras around the streets to transmit the pictures, and (b) iteratively allowing a vehicle with a camera covering the most amount of uncovered direction to transmit until the sufficient condition is met. In this way, we can minimize the network traffic effectively. The format of the report message from vehicle to cloud, denoted by $M_R$ is given by: $M_R = (\text{timestamp}|\text{loc}_V|\text{loc}_e|\text{Pic.Data}|PS_{V_i}^t|\text{Contents})K_2^C$.

$\text{timestamp}$ is the message sending time and is assumed to be closed to the event time (but not necessarily), $\text{loc}_V$ is the location of the mobile observer and $\text{loc}_e$ is the location of the event. The whole report is sent to cloud anonymously with pseudonym $PS_{V_i}^t$ by vehicle $V_i$ and for integrity check and loose authentication; vehicle $V_i$ also includes the hash value of the contents, calculated with its individual secret key $K_{V_i}$. The whole message is encrypted with the cloud’s public key so that the content and the pseudonym cannot be abused by the adversaries. Cloud stores these reports in the database and indexes them with the event time. Whenever an investigation is going on, cloud dispatcher provides the information to the revocation authorities for the specified time interval.

C. Identity Exchange

When a vehicle wants to exchange its pseudonym for privacy preservation, it shows its intention in its beacon messages. We include an $\text{intent}$ flag in the beacon message that shows the intent of the vehicle for exchanging pseudonyms. The neighbors who receive that beacon have the choice if they want their pseudonyms to be exchanged or not. The generic beacon denoted by $M_b$ will look like: $M_b = (B_{data}|\text{Sec.Primitives}|\text{intent})$. We do not outline the exact details of the exchange but the requirements that must be fulfilled prior to pseudonym exchange are anonymous mutual authentication of the exchanging entities, non-repudiation, privacy preservation, pseudonym validity, and verification. Kim et al.’s scheme is the most suitable scheme for pseudonym exchange in our proposed scheme [18]. We assume their scheme to be used in our pseudonym exchange. Their scheme fulfills all aforementioned security primitives. It is worth noting that before exchanging pseudonyms, vehicles would periodically receive PRL (Pseudonym Revocation List) from RSUs and check for the pseudonym validity beforehand. And we also assume that the exchange report is sent to RAs anonymously. RAs maintain another database for the exchange history referred to as PEHT (Pseudonym Exchange History Table) which contains time of the exchange, the source pseudonym and the destination pseudonym. This exchange information is used for revocation purpose which is explained in the next subsection in detail. The format of PEHT maintained by RAs is shown in Fig. 3.

D. Revocation

In order to proceed with revocation, RAs retrieve the forensics from the cloud. When queried based on a time interval, cloud provides RAs with the data related to that time interval. 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 to through the pseudonym exchange history table (PEHT) to figure out whether the pseudonym has been used by its original owner 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: $PS_{V_i}^t = c_2 \oplus H(sc_1) = (K_i||K_{V_i}) \oplus H(rPub) \oplus H(rsPub)$.

When RAs decrypt the keys $K_i$ and $K_{V_i}$, then revocation is almost done, all RAs have to do is to decrypt $a$ and then extract VID from the pseudonym. In our proposed scheme, we use back search in PEHT with respect to time and consider
only the latest best match with the pseudonym in question. In order to understand how PEHT helps in singling out the sender of the message with exchanged pseudonym (even in case of multiple exchanges), we give the following example. Let us suppose there are 4 cars A, B, C, and D. The cars have pseudonyms \{PS^1_A, PS^2_A, ..., PS^n_A\}, \{PS^1_B, PS^2_B, ..., PS^n_B\}, \{PS^1_C, PS^2_C, ..., PS^n_C\}, and \{PS^1_D, PS^2_D, ..., PS^n_D\}. For the ease of understanding, let us suppose the pseudonym exchange took place according to Fig. 4. It can be seen that at time \(t_1\), A received \(PS^2_B\) from B for an exchange of \(PS^3_A\). That means vehicle A is using \(PS^3_A\). If a message with \(PS^3_A\) is under observation at time \(t_1\), then vehicle A must be held responsible for that, not vehicle B. However, at time \(t_3\), vehicle B exchanges \(PS^3_A\) (originally owned by vehicle A) with C’s pseudonym \(PS^3_C\). At this point in time if the message under observation after \(t_3\) contains \(PS^2_A\), vehicle C must be held responsible. Hence the current sender of the pseudonym is traced by RAs.

V. Evaluation

A. Security Analysis

In order to function properly, our proposed pictorial service must be secure. We assume a passive adversary where he/she can overhear the transmission between the vehicles and cloud service provider, and can analyze it. The adversary is, however, not able to follow the pseudonym exchange, because the exchange messages are sent anonymous and encrypted [18]. In a broader picture, beaconing mechanism must be secure at par as well since the intent for pseudonym exchange is broadcasted through beacon messages. However we assume that there is a secure beaconing mechanism already in place. The first and basic security requirement is the authenticity and integrity of content of the picture. The content of the picture must be authentic, securely transferred to the cloud and non-repudiated. Data integrity is guaranteed with the help of hash function; however we used keyed hash with user individual secret key \(K_{Vi}\) which gives twofold advantages: it guarantees data integrity of the report and it also guarantees non-repudiation because only the sender holds \(K_{Vi}\) and nobody else, unless and until \(K_{Vi}\) is compromised, otherwise. The effect of keys compromise is critical for our proposed scheme. However the compromise of \(K_i\) alone does not have severe consequences because the adversary can get only \(\alpha\) which is a part of pseudonym. In the worst case if both \(K_i\) and \(K_{Vi}\) are compromised, then the consequences will be dire. In such case the adversary not only has the actual pseudonym, but also can manipulate or reuse it.

B. Conditional Privacy

By exchanging pseudonyms, the report becomes more ambiguous and hard to link to the owner and/or the current user of the pseudonyms. Nevertheless, as a trapdoor, we include the hashed \(VID\) in the pseudonym, however that is based on the argument that \(K_{Vi}\) is not compromised, our argument does not hold otherwise. To measure the privacy of the node, we measure the anonymity of the reporter by calculating entropy denoted by \(H\). To calculate the entropy, we assume that the anonymity set is the set of the users around the SoI denoted by \(V\) and let \(p_{Vi}\) be the probability that the node \(Vi\) be the target witness where \(\forall Vi \in V, \sum_{i=1}^{\mid V\mid} p_{Vi} = 1\). The entropy \(H\) of the target user \(Vi\) in the anonymity set \(V\) is given by: \(H = -\sum_{i=1}^{\mid V\mid} p_{Vi} \times \log_2 p_{Vi}\). Since our anonymity set is \(V\), the possible outcomes can be \(\mid V\) assuming the fair distribution and the probability of each outcome will be \(\frac{1}{\mid V\}}\). If the distribution is normal and the occurrence of the nodes to be related to the pseudonyms in question is equally likely, then the maximum entropy is also given by the following formula: \(H_{max} = -\sum_{i=1}^{\mid V\mid} p_{Vi} \times \log_2 p_{Vi} = \log_2 \mid V\}.\)

It must be noted that in such case, the normal entropy is equal to the maximum entropy, i.e. \(H = H_{max}\). However due to the ephemeral nature of VANET, the situation where \(H\) equals to \(H_{max}\), is hard to achieve.

C. Revocation

The maintenance of PEHT is critical in our proposed scheme because it leads us to the original sender of the pseudonym. One unique feature of our proposed scheme is that the same pseudonym can be used simultaneously by both the owner and the exchanger and still be subject to revocation. Additionally, one vehicle can either exchange its own pseudonym or an already exchanged pseudonym with somebody else. This can go to a deeper level, but that is not an issue for our proposed scheme as long as the PEHT is implemented. There are two scenarios to consider: 1) If the pseudonym is exchanged with a number of users and they do not use it simultaneously, we call the revocation as direct revocation where only the sender of the pseudonym is singled out by the RAs through searching records in PEHT, colluding, constructing \(s\) from \(s_i\) and then extracting \(VID\) from the pseudonym. 2) When the owner of the pseudonym uses its pseudonym even after exchanging it with its neighbor simultaneously. In that case, the revocation is referred to as indirect revocation. The node with whom the pseudonym has been exchanged, can be revoked through direct revocation. For the owner of the pseudonym, in the first step, the possible targets are reduced to those who currently possess the pseudonym in question and then the hash value included in the pseudonym is used to reach the owner of the report who used the pseudonym, and that is the potential owner of the pseudonym as well.

D. Computation and Communication Overhead

We believe that because of the different frequencies of DSRC (Dedicated Short Range Communication) and 3G/4G, a normal distribution of both aforementioned standards would produce better results in terms of communication overhead and the number of nodes using aforementioned standard for VWaaS is an important factor. Dividing the communication...
overhead over DSRC and 4G would reduce the channel saturation problem and increase the throughput. Now we consider the computational overhead. In order 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. The cost of revocation is divided into two scenarios depending upon the usage of pseudonyms, i.e. direct and indirect revocation.

In case of direct revocation, the cost denoted by $T_{dir-rev}$ is given by:

$$T_{dir-rev} = Cost(\text{SearchTable}_{pseudo} + \text{PEHT}) + Cost(\text{Extract}K_{\text{V}}, R_{\text{V}}) + Cost(\text{Symm.Decryption}) = 2T_{\lambda} + 2T_{\text{mul}} + 2T_{H} + 2T_{\text{sym-dec}}.$$  

$T_{\lambda}$ is the time incurred by the table search ($\text{Table}_{pseudo}$-pseudonym table and PEHT), $T_{\text{mul}}$ is the time required for point multiplication, $T_{H}$ is the time required to calculate hash, and $T_{\text{sym-dec}}$ is the time required for symmetric decryption.

In case of indirect revocation, RA has to examine all the current holders of the pseudonym in question that was used simultaneously. The revocation in such case consists of two steps: single out the nodes that possessed and used the pseudonym and then compare their $h_{K_{\text{V}}}()$ value with the pseudonym in question. The revocation cost of the indirect revocation denoted by $T_{indir-rev}$ is given by:

$$T_{indir-rev} = 2T_{\lambda} + 2\sum_{i=1}^{J}(T_{\text{mul}} + T_{H} + T_{\text{sym-dec}}) + \sum_{i=1}^{J}T_{h_{\lambda,k}}.$$  

$T_{h_{\lambda,k}}$ is the time required for keyed hash calculation and in case of indirect revocation, RAs have to examine $j$ number of nodes.

**Running Time:** In order to cover the 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 [16], the total running time is polynomial function of $V$ where $V$ is the total number of vehicles. It must be noted that in SoI, the full view finding method requires $O((k + l)^{2})$ where $(k + l) \leq V$, $k$ is the number of vehicles in SoI and $l$ is the number of fixed roadside cameras.

**VI. CONCLUSION**

In this paper, we proposed VWaaS (Vehicles Witnesses as a Service) in VANET-based clouds. In the proposed scheme, vehicles on the road with the help of cameras mounted on them along with fixed cameras, take pictures of any incident taken place in their vicinity and send the pictures to the cloud. Cloud, on the other hand, provides the stored forensic evidences to the law enforcement or insurance agencies for investigation. We provide conditional anonymity to the vehicles that contribute to this service. Our proposed scheme has a particular significance in case law and order situation where original forensic evidences must be acquired from the scene, and in order to avoid framing benign vehicles, for instance in case of a terrorist attack or a deadly accidents.

**ACKNOWLEDGMENT**

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2012-R1A2A2A01046986). This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-R1A1A2009152).

This work was supported in part by US National Science Foundation (NSF) CREST No. HRD-0833184 and by US Army Research Office (ARO) No. W911NF-0810510.

**REFERENCES**


