Journal of Universal Computer Science, vol. 19, no. 16 (2013), 2385-2403
submitted: 15/7/13, accepted: 27/9/13, appeared: 1/10/13 © *J.UCS*

A Privacy Preserving Message Delivery Protocol Using Identity-Hidden Index in VDTNs

Youngho Park, Chul Sur, Sanguk Shin, Kyung-Hyune Rhee[1]
(Department of IT Convergence Application Engineering
Pukyong National University, Busan, Republic of Korea
{pyhoya, kahlil, shinsu, khrhee}@pknu.ac.kr)

Changho Seo
(Department of Applied Mathematics, Kongju National University
Gongju-Si, Chungcheongnam-Do, Republic of Korea
chseo@kongju.ac.kr)

Abstract: Vehicular Delay Tolerant Networks (VDTNs) are characterized model of Vehicular Ad Hoc Networks where vehicles disseminate messages through fixed relay nodes placed on roadside by utilizing a store-carry-forward method. In this paper, we propose a secure message delivery protocol for protecting receiver-location privacy in socialspot-based VDTN because location privacy is one of the most important security requirements. To design a simplified protocol, we eliminate the use of conventional pseudonym-based vehicle identification accompanied with a complex pseudonymous certificate management. Instead, we introduce an identity-hidden message indexing which enables a receiver vehicle to query a message whose destination is itself to the socialspot RSU without revealing its identity, and we make use of non-interactive key agreement scheme to establish a secure communication channel between message source and destination vehicles. Furthermore, we demonstrate experimental results to confirm the reduced cryptographic overhead and the effectiveness of privacy preservation for the proposed protocol.
Key Words: VANET, VDTN, privacy preservation, ID-hidden index, authentication
Category: C.2.0, L.7

1 Introduction

Vehicular Ad Hoc Networks (VANETs) are emerging type of networks on the basis of incorporating advanced car technology with wireless communications to enable various useful applications on the road. Typically, modern vehicles will equip with an on-board unit (OBU) communication device, which allows Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications with other vehicles as well as a road-side unit (RSU). Hence, VANETs have recently become one of the promising wireless networking research areas to support Intelligent Transportation Systems and Telematics. This trend is due to Dedicated Short Range Communications (DSRC) [Kenney 2011] and the GPS-based navigation system with digital map. With these deployments, such VANETs enable useful

[1] Corresponding author.

applications in our daily lives such as not only cooperative driving safety and probing vehicle data for better driving comfort but also infotainment services by vehicular communications.

However, an end-to-end communication path between vehicles may not exist unfortunately because vehicles are constantly moving with frequently changing road segments [Wang and Li 2009, Allal and Boudjit 2013] which, in turn, it makes network connectivity unreliable. As a promising solution to this challenge, for non-realtime constrained VANET applications, a store-carry-forward paradigm is considered to deliver a message to a remote destination vehicle effectively by the socialspot tactic [Lu et al. 2010a] in city road environments. Here, the socialspots are referred to the locations in a city road that many vehicles often visit such as intersections around famous shopping malls, restaurants, or cinemas. It is viable to adopt RSU assisted message forwarding mechanism in a VANET in which RSUs are deployed to help message relays. Hence, we can utilize an RSU installed in the socialspot as a relay node for message forwarding in an opportunistic way. So, the behavior of such VANET communications can be modeled as a Delay Tolerant Network known as Vehicular Delay Tolerant Networks (VDTNs) [Pereira et al. 2012], and packet forwarding protocols exploiting store-carry-forward manner have been proposed [Zhao and Cao 2006, Jeong et al. 2011].

Although VANETs have received a lot of attention, there are still some prerequisite challenges need to be resolved before VANET services become reality. One of the challenging issues is security and, in especial, privacy of vehicles or drivers has become one of the most concerns for the successful deployment of VANETs. In the same vein, socialspot-based VDTN applications must protect vehicle's privacy even though the locations of socialspots for message dissemination are known publicly [Lu et al. 2010a, Lu et al. 2010b, Lin et al. 2011]. That is, a security mechanism should be able to make it difficult as far as possible for an adversary who knows the locations of socialspots to infer which vehicle receives a message from the RSU at each socialspot.

1.1 Related Work

A variety of secure vehicular communication protocols have been proposed for the last decade, and most of existing protocols mainly focus on privacy-preserving authentication for cooperative driving safety applications within one-hop communication range[Raya and Hubaux 2007, Lu et al. 2008, Jung et al. 2009]. For multi-hop forwarding applications, secure routing protocols for VANET have been proposed [Kim et al. 2008, Yang et al. 2010] but these existing protocols assume that vehicles are well connected for hop-by-hop packet forwarding. As an alternative, epidemic routing [Zhang et al. 2007] mechanism using flooding technique is regarded as an intuitive solution to protect receiver's location privacy in VANET. However, flooding technique results in a large number of duplicate packets in the network and, as a result, it is inefficient.

On research on socialspot-based secure message delivery in recent, Lu et al. proposed a socialspot tactic privacy-preserving data forwarding protocols in [Lu et al. 2010a] and [Lu et al. 2010b] in order to protect receiver-location privacy. Those protocols are on the basis of pseudonym-based vehicle identification for anonymous message delivery and receiver authentication. Therefore, each vehicle has to have pre-loaded pseudonym-set for avoiding vehicle tracking by periodically changing its pseudonym on the road. However, they require complex pseudonym-based cryptographic key management depending on the number of pre-loaded pseudonyms, and all vehicles must know receiver vehicle's pseudonym to send a message to the receiver. On the other hand, the authors [Lu et al. 2010b] incorporated conditional privacy-preserving authentication based on group signature and universal re-encryption scheme with packet forwarding protocol for protecting vehicle's location privacy from packet analysis attack. However, when a receiver vehicle downloads a message it is required for the receiver to perform a complex mutual authentication process with RSU at the socialspot due to the much time consuming operation of group signature scheme [Lu et al. 2008, Park et al. 2010].

What is worse, the protocol of [Lu et al. 2010b] only considers the stationary receiver so it is possible that receiver's fixed location will be exposed to an adversary, and the protocol of [Lu et al. 2010a] does not provide message source authentication so this protocol cannot guarantee the non-repudiation if a malicious vehicle sends a bogus message.

1.2 Contribution and Organization

The complexity of previous protocols is caused by the use of pseudonyms instead of real identity of vehicles to specify message source and destination during message forwarding protocol. Those require high cost cryptographic schemes combined with pseudonymous keys for the purpose of providing privacy-preserving authentication and identity unlinkability. Based on the above observation, in this paper, we propose a socialspot-based secure message delivery protocol for preserving receiver-location privacy. The main design goal of this paper is to simplify the cryptographic operation for privacy preserving message delivery between a socialspot RSU and a receiver vehicle by eliminating the use of pseudonym-set accompanied with pseudonym certificate management.

The contributions of this paper are threefold. First, instead of putting vehicles' pseudo-ID to identify a receiver vehicle in anonymous manner, we put forth an identity-hidden message indexing in order for a receiver vehicle to retrieve the message bound for it from the socialspot RSU without revealing its identity. Second, we establish a unidirectionally authenticated secure message delivery channel from a sender to a receiver for VDTNs in which an interactive message exchange is not always possible because of no simultaneous end-to-end connection. For anonymous authentication of a receiver vehicle to a socialspot RSU without presenting receiver's identity-related information, thirdly, we make the receiver vehicle be implicitly authenticated to the RSU by proving knowledge of the shared secret key with the sender. Then the RSU makes sure that the receiver is the specified vehicle of the message sender.

In the early version of this paper [Park et al. 2013], we only sketched the protocol without apparent evaluation results. We demonstrate the efficiency of the proposed protocol by evaluating the message processing delay, and show that it is hard for an adversary to link a specific vehicle ID to a message index at a socialspot by estimating the index finding probabilities in city road environments.

The remainder of this paper is organized as follows. In Section 2, we describe our system model and security goals considered in this paper. We present the proposed protocol in Section 3, and discuss and analyze the protocol in terms of security and efficiency in Section 4, respectively. Finally, we conclude this paper in Section 5.

2 System Model and Design Goals

VDTNs are characterized networks of VANETs where vehicles communicate with each other and with fixed nodes placed along the roads in order to disseminate messages [Pereira et al. 2012]. Some of potential applications for these kind of networks are to establish a location-based social network to help users who have common favorites to share some interesting information in a temporally virtual community on the road [Smaldone et al. 2008] such as notification of traffic conditions and road accident warnings, weather reports, advertisements and so on.

In this section, we describe a socialspot-based message delivery for VDTNs and security goals of the proposed protocol. We assume vehicles communicate with each other and find their neighboring vehicles through beacon messages according to the DRSC specification, and vehicles are equipped with pre-loaded digital map incorporating with a GPS system. We consider the system model which consists of vehicles equipping with OBUs, RSUs installed in socialspots and Trusted Authority(TA) for security management as shown in Figure 1, respectively.

- TA is in charge of issuing ID-based private keys to the registered vehicles and RSUs, and provides public system parameters for running security protocol.
- Socialspots denoted as $\mathcal{SS} = \{ss_1, ..., ss_l\}$ are referred to as roads or intersections around which many vehicles will visit, for example, famous shop-

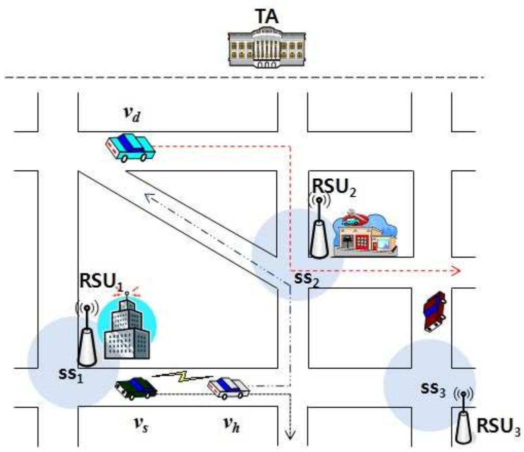


Figure 1: System model for socialspot-based VDTN.

ping malls, movie theaters, and such like. At each $ss_j \in \mathcal{SS}$, a huge-storage possessing RSU_j subordinated by the TA is installed so that RSU_j can temporarily store some messages forwarded to the receiver vehicles passing through the ss_j.

– Each vehicle $v_i \in \mathcal{V} = \{v_1, ..., v_n\}$ registered to the system equips with OBU for V2V and V2I communications, and cooperates with each other in delivering a message for a socialspot in store-carry-forward manner.

In those settings, message forwarding strategy from a sender vehicle to a destination socialspot can be divided into the following two methods; 1) If the sender vehicle directly passes the socialspot, the sender immediately carries the message and then forwards it when it arrives on the socialspot. 2) Otherwise, some vehicles driving toward the socialspot cooperates for store-carry-forward message delivery.

As an example scenario in Figure 1, suppose that v_s wants to send a message msg to v_d which will visit socialspot ss_2 later, but v_s does not drive toward the socialspot directly.

1. At time t_1, v_s asks v_h which drives toward the ss_2 for forwarding the msg.

2. v_h carries the msg and arrives on the socialspot ss_2 at time t_2 ($t_2 > t_1$), then forwards the msg to the RSU_2.

3. When v_d passes the ss_2 at time t_3 ($t_3 > t_2$) while RSU_2 stores the msg, v_d requests msg bound for it then RSU_2 provides v_d with msg.

In such a VDTN scenario, we consider the following security goals to design a secure message delivery protocol against a global passive adversary $\mathcal{A}$. The adversary $\mathcal{A}$ can overhear V2V and V2I communications, but cannot compromise any vehicle (or RSU) and access the internal information of them. Thus, $\mathcal{A}$ tries to identify vehicles or to trace the location of a vehicle by packet analysis.

– *Anonymous Channel* : An adversary $\mathcal{A}$ cannot identify the message sender and receiver from eavesdropping on the message delivery protocol.

– *Authentication* : Only a valid receiver vehicle specified by a sender can retrieve the message whose destination is itself by authenticating itself to the RSU at a socialspot.

– *Receiver Privacy* : Even though the location of a socialspot is known, it is hard for an adversary $\mathcal{A}$ to infer which vehicles retrieved messages at the socialspot.

3 Proposed Protocol

To design the proposed protocol, we make use of ID-based non-interactive key agreement scheme [Sakai et al. 2000, Dupont and Enge 2006] (but the IDs of vehicles are not included in message delivery protocol) to establish a secure channel between sender and receiver vehicles, and cryptographic hash function to generate an identity-hidden message index while binding a specific receiver vehicle at a socialspot is possible. Table 1 describes the notations used in the proposed protocol.

Table 1: Notations and descriptions.

notation	description
$params$	public system parameters
SK_i	ID-based private key of an entity i
k_{ij}	shared secret key between i and j
T	valid time period of a message
$Enc_k(\cdot)$	encryption under key k
$Dec_k(\cdot)$	decryption under key k
$Sig_{SK_i}(\cdot)$	ID-based signature under signing key SK_i
$Vrf_i(\cdot)$	ID-based signature verification for a given ID i
$h(\cdot)$	cryptographic hash function
$MAC_k(\cdot)$	message authentication code under key k

The proposed protocol consists of *setup*, *message constitution*, *message forwarding*, and *message retrieving* phases. TA issues ID-based cryptographic quantities in the setup phase. Then, a message sender can establish a shared secret key with a receiver non-interactively and constitute a secure message package delivered to a receiver through a socialspot RSU. In order to retrieve a message for a valid receiver, the receiver must show knowledge proof for the secret key shared with the message sender to a socialspot RSU in message retrieving phase.

3.1 Setup

The TA configures system parameters for bilinear map [Boneh and Franklin 2003] in the setup phase and issues ID-based private keys to the registered RSUs and vehicles as initial setup and registration procedure. At this phase, geographic location information or road identifier of a socialspot can be used as RSU's ID (i.e., ss_j) for key generation.

setup and registration procedure
1. TA chooses bilinear map groups $(\mathbb{G}, \mathbb{G}_T)$ of the same prime order q and a random generator $P \in \mathbb{G}$, and 2. chooses a random number $s \in \mathbb{Z}_q^*$ as its master secret key and sets the corresponding public key $P_0 = sP$, and 3. configures public system parameters $param = \langle \mathbb{G}, \mathbb{G}_T, q, \hat{e}, P, P_0, H_1, H_2 \rangle$, where $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a bilinear map, $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ are cryptographic hash functions, respectively. 4. For each $v_i \in \mathcal{V}$ and each RSU_j at $ss_j \in \mathcal{SS}$, TA issues ID-based private keys $SK_{v_i} = sH_1(v_i)$ for v_i and $SK_{ss_j} = sH_1(ss_j)$ for RSU_j, respectively.

3.2 Message Constitution

When a vehicle v_s wants to send a message msg to a receiver vehicle v_d which will pass a socialspot ss_j sometime, v_s executes the message constitution procedure to make a secure message package, M, encapsulated as shown in Figure 2. In this message formation, source ID and receiver ID are encrypted under the non-interactively shared key between sender and receiver but message delivery information such as socialspot ID and message index are placed in encapsulated message header by sender vehicle.

In step 1 of message constitution procedure, k_{sd} and k_{sj} are non-interactively shared keys with a receiver vehicle v_d and with a socialspot RSU_j, respectively. Here, key k_{sd} is used for encrypting the message delivered to v_d, and k_{sj} for checking message integrity by RUS_j. The identity-hidden message index I in

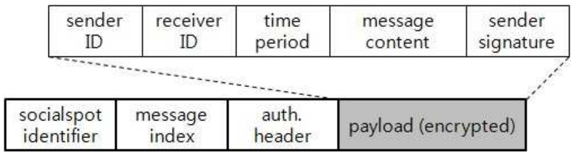


Figure 2: Message format for secure message delivery through a socialspot.

step 4 will be used for a receiver vehicle to query a message for it in the message retrieving phase. In addition, $\{P_s, W\}$ in authentication header field will be used by RSU_j to check the knowledge proof given by a receiver vehicle for the shared key k_{sd} between the sender v_s and the receiver v_d.

---

message constitution procedure

---

1. v_s chooses a random number $r \in \mathbb{Z}_q^*$, and generates $k_{sd} = \hat{e}(rSK_{v_s}, H_1(v_d))$ and $k_{sj} = \hat{e}(rSK_{v_s}, H_1(ss_j))$.
2. v_s computes $P_s = rH_1(v_s)$, $w = H_2(k_{sd}|T)$, and $W = w^{-1}P$.
3. v_s generates $C = Enc_{k_{sd}}(v_s|v_d|T|msg)$ and $\sigma = Sig_{SK_{v_s}}(v_s|v_d|T|msg)$, where σ is sender v_s's ID-based signature [Cha and Cheon 2003].
4. Then, v_s constitutes the encapsulated message $M = \{ss_j, I, P_s, W, C|\sigma, chk\}$ forwarded to the destination socialspot ss_j as follows:
   - msg.index : $I = h(v_d, ss_j, T)$
   - auth. header : $\{P_s, W\}$
   - payload : $\{C \mid \sigma\}$
   - $chk = MAC_{k_{sj}}(ss_j, I, P_s, W, C|\sigma)$

3.3 Message Forwarding

Once the encapsulated message M is constituted, M can be delivered to a destination socialspot ss_j according to the following message forwarding strategy. At this phase, we assume a packet forwarding protocol for store-carry-forward fashion, such as VADD [Zhao and Cao 2006] and TBD [Jeong et al. 2011], with collaboration of volunteer vehicles. As mentioned in Section 2, if the sender vehicle passes the socialspot, the sender will carry the message and then forward it when it arrives on the socialspot. Otherwise, some vehicles driving toward the socialspot will cooperate for store-carry-forward message delivery.

When the message M ultimately reaches RSU_j at ss_j by using the message forwarding strategy, RSU_j temporarily stores $\{I, P_s, W, C|\sigma\}$ while a receiver vehicle related to the message index I requests the message as passing by it. Note that the main goal of this paper is to protect receiver's privacy from an adversary, we do not consider compromising of vehicles and message forgery attack by an active adversary during the message forwarding.

message forwarding strategy
1. if v_i passes a socialspot ss_j then carries the message M to ss_j
2. else v_i asks collaboration of nearby vehicles while driving toward ss_j and
3. if v_i detects a volunteer vehicle $v_h \in \mathcal{V}$ then
4. v_i forwards the message M to the v_h
5. $v_i \leftarrow v_h$ and go to 1
6. end if
7. end if
8. on arriving at ss_j, v_i forwards the message M to RSU_j
9. if RSU_j receives the M
10. computes key $k_{sj} = \hat{e}(P_s, SK_{ss_j})$ from P_s in M and
11. if $chk \stackrel{?}{=} MAC_{k_{sj}}(ss_j, I, P_s, W, C\|\sigma)$ holds then stores $\{I, P_s, W, C\|\sigma\}$
12. end if

3.4 Message Retrieving

When a vehicle v_d goes by a socialspot ss_j on its way driving, v_d can get a message M whose destination is itself according to the following protocol steps. Figure 3 briefly depicts the overall message retrieving protocol between a receiver vehicle and a socialspot RSU.

1. v_d, as expecting a message for it on RSU_j's storage, generates its message index at ss_j as $I = h(v_d, ss_j, T)$, then queries I to RSU_j.
2. RSU_j searches its storage for the message corresponding to I. If the message is found, RSU_j sends P_s of matching index I to v_d as a challenge for authentication.
3. Upon receiving P_s, v_d computes the secret key $k_{sd} = \hat{e}(P_s, SK_{v_d})$ shared with a sender and $w = H_2(k_{sd}|T)$, then gives $\widetilde{W} = wP$ to the RSU_j as a proof of knowledge of the shared key.

4. With W sent from a sender v_s and $\widetilde{W}$ from v_d, RSU_j checks if $\hat{e}(W, \widetilde{W}) \stackrel{?}{=} \hat{e}(P, P)$ to verify the proof of knowledge. If the verification holds, RSU_j authenticates v_d as a valid receiver specified by the sender, then provides $\{C|\sigma\}$ to v_d.

5. v_d recovers $\{v_s|v_d|T|msg\}$ from the payload by decrypting $Dec_{k_{sd}}(C)$, and finally completes the message retrieving protocol after verifying the signature σ as $Vrf_{v_s}(\sigma)$.

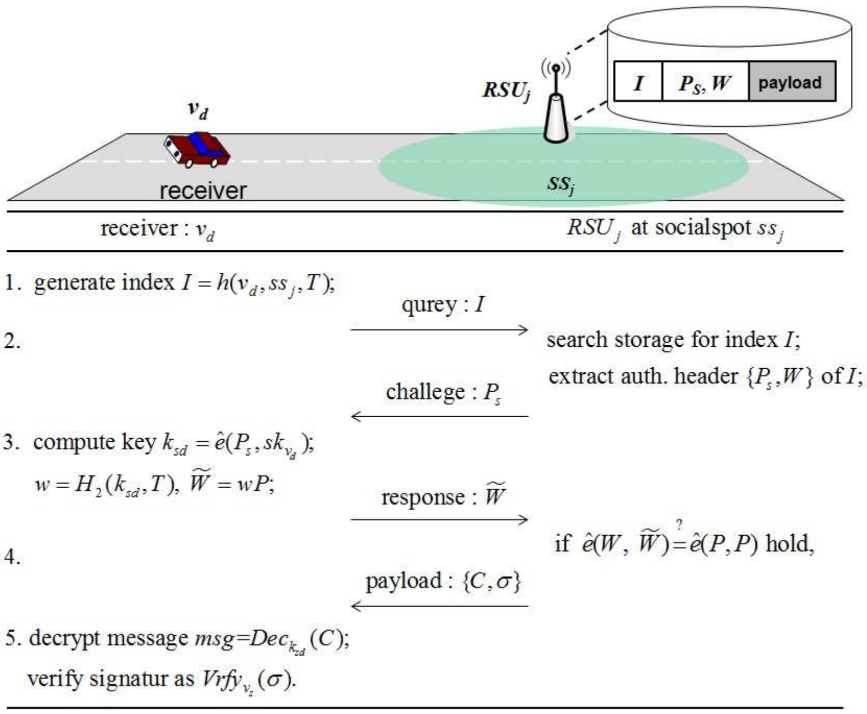


Figure 3: Message retrieving protocol of a receiver vehicle at a socialspot.

4 Analysis

In this section, we give analysis of the proposed protocol in terms of security and efficiency for privacy preserving message delivery through a socialspot RSU. Table 2 compares functional features of the proposed protocol with Lu et al.'s [Lu et al. 2010a]. The remarkable distinction of the proposed protocol is eliminating the use of pseudonyms in privacy-preserving secure message delivery protocol as well as providing end-to-end authentication between a sender and a receiver. Hence, Lu et al.'s protocol burdens additional pseudonym management overhead but ours does not. We will show the efficiency of the proposed protocol in the following subsection. Relating to cryptographic overhead in Table 2, t_p and t_m are bilinear pairing and scalar multiplication in $\mathbb{G}$, respectively, for processing security protocol with an RSU at a socialspot.

Table 2: Comparison of the proposed protocol.

	Lu et al.	proposed
adversary	passive	passive
authentication	receiver auth.	sender/receiver auth.
anonymity	pseudonym set	ID-hidden index
crypto. cost	$3t_p + 2t_m$	$2t_p + 1t_m$

4.1 Efficiency of message retrieving

One contribution of the proposed protocol is a simplified authentication process with no use of pseudonymous keys for message retrieving from a socialspot RSU. To show the reduced cryptographic overhead, we evaluated and compared the processing delay of message retrieving protocol with Lu et al.'s using the analytic model as shown in Figure 4.

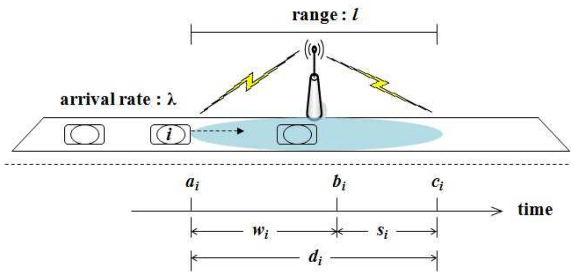


Figure 4: Processing delay model for message retrieving service at a socialspot.

We assumed that RSU's service discipline is first-come-first-served and a job in service is non-preemptive. Suppose that arrival time of a requesting vehicle v_i is a_i with an exponential random variable of arrival rate λ. The job for v_i begins service at b_i after waiting in the queue for $w_i = b_i - a_i$, and then completes message retrieving service at c_i after taking s_i service time. Hence, the processing delay d_i of message retrieving service for v_i can be measured by $d_i = w_i + s_i$.

To measure the processing delay, we estimated cryptographic overhead by using pairing-based cryptography library of [PBC] on Pentium-III 1GHz machine, and inter-arrival time of vehicles was generated from exponential distribution with λ. We simulated the delay model and traced processing delay of each vehicle whose arrival rate is empirically $\lambda = 1.0$ assumed for simulation, and Figure 5 shows the results. From this result, we can observe that the proposed protocol suffers from shorter processing delay than Lu et al.'s for over 250 cumulated services due to our simplified authentication.

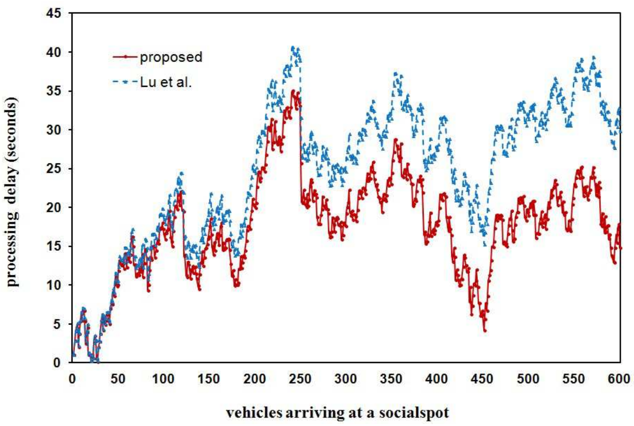


Figure 5: Message retrieving delay for arrival rate $\lambda = 1.0$.

In addition, we also evaluated successful message retrieving ratio considering vehicle's moving speed for passing the socialspot. Let l and v be RSU's transmission range and moving vehicle's speed, respectively. The processing delay must be $d_i \leq l/v$ because the service has to be completed before a moving vehicle v_i goes out of RSU's range to receive a message properly from the RSU. Figure 6 shows the valid message retrieving service ratio for various vehicle's moving speed from 30km/hr to 110km/hr (that is, 8m/s - 30m/s) for passing RSU's range $l = 1,000m$. We can also observe that Lu et al.'s service ratio drastically decreases if vehicles move faster with over 70km/hr speed while the proposed protocol can serve almost all requests.

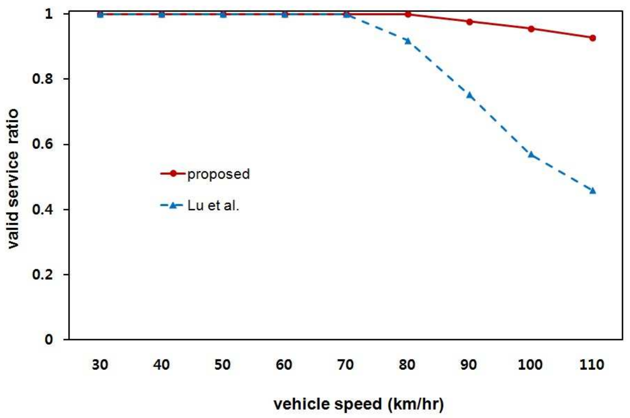


Figure 6: Valid message retrieving service ratio depending on vehicle speed.

4.2 Security

The security of the proposed protocol entirely depends on the non-interactive key agreement scheme and cryptographic hash function. We will focus on how the proposed protocol can fulfil our security goals under our adversary model.

4.2.1 Anonymous channel

In the proposed protocol, the delivered message content $\{v_s|v_d|T|msg\}$ from a sender v_s to a receiver v_d is encrypted under non-interactively shared key k_{sd}, i.e., $C = Enc_{k_{sd}}(v_s|v_d|T|msg)$. Hence, when we assume the secrecy of non-interactive key agreement scheme [Dupont and Enge 2006], it is difficult for an adversary $\mathcal{A}$ to identify sender and receiver from eavesdropping on the message transmission. Even if $\mathcal{A}$ can know that the destination of the encapsulated message is a socialspot ss_j, $\mathcal{A}$ cannot capture the identities of vehicles which retrieve messages through the socialspot RSU_j because no vehicle identity is presented to the RSU_j. Therefore, the proposed protocol can guarantee the anonymity of message transmission.

In addition, Kate et al. [Kate et al. 2010] presented that they could construct an onion routing for anonymity network on the basis of non-interactive key agreement scheme. If we encrypt the encapsulated message M again under key k_{sj} instead of $MAC_{k_{sj}}$ in message constitution phase, the path $v_s \rightarrow \ldots \rightarrow RSU_j \rightarrow v_d$ can be regarded as an onion path based on Kate et al.'s observation.

4.2.2 Authentication

In order to obtain a message temporarily stored in an RSU_j in message retrieving phase, a receiver vehicle must be authenticated to the RSU_j which checks if the requesting vehicle is the designated receiver by a sender vehicle. In our protocol, for a vehicle v_d to be authenticated as a valid receiver, v_d should present the proof of knowledge $\widetilde{W} = H_2(k_{sd}|T)P$ for the secret key k_{sd} shared with a sender v_s. The consistency of the keys $k_{sd} = \hat{e}(rSK_{v_s}, H_1(v_d))$ generated by v_s and $k'_{sd} = \hat{e}(P_s, SK_{v_d})$ by v_d can be proven as $\hat{e}(rSK_{v_s}, H_1(v_d)) = \hat{e}(rH_1(v_s), sH_1(v_d)) = \hat{e}(P_s, SK_{v_d})$. Therefore, only the v_d bound in the non-interactively shared secret key k_{sd} by sender v_s can response the correct proof of knowledge and be authenticated as valid receiver.

Only if the verification of $\hat{e}(W, \widetilde{W}) = \hat{e}(P, P)$ holds, RSU_j will send $\{C|\sigma\}$ to v_d as regarding v_d is the receiver who can agree with the message sender. Then, v_d can recover original message $\{v_s|v_d|T|msg\}$ by decrypting C, and authenticates the sender v_s as verifying v_s's signature σ.

4.3 Receiver privacy

As mentioned before, the proposed protocol does not put vehicle's identity for message transmission nor receiver's identity is given to the RSU_j at a socialspot ss_j in message retrieving phase. Instead, a receiver v_d can be bound by identity-hidden message index $I = h(v_d, ss_j, T)$ which is the result of cryptographic one-way hash function. Therefore, it is hard for an adversary $\mathcal{A}$ to decide which vehicle receives a message from I at the socialspot even though the location of the socialspot is publicly known.

Moreover, we can generate a different message index I' ($\neq I$) for different time period or different socialspot, i.e., $I' = h(v_d, ss_j, T')$ for $T' \neq T$ or $I' = h(v_d, ss_k, T')$ for $ss_j \neq ss_k$, due to the functionality of cryptographic hash function. Hence, the proposed protocol can guarantee the unlinkability for a receiver vehicle because it is infeasible for $\mathcal{A}$ to distinguish that the given indexes I' and I are linked to the same receiver.

However, one feasible attack for $\mathcal{A}$ is to prepare possible message index set $\mathcal{I}_S$ for a socialspot ss_j from arbitrarily chosen vehicles identities $\mathcal{V}_A = \{v_1, ..., v_m\}$ for a given time period T at a specific socialspot ss_j such that $\mathcal{I}_S = \{h(v_i, ss_j, T)|v_i \in \mathcal{V}_A\}$, and observe if an index $I = I' \in \mathcal{I}_S$ occurs at the socialspot ss_j or not. If it occurs, then $\mathcal{A}$ can decide the matching identity $v_i \in \mathcal{V}_A$ such that $I' = h(v_i, ss_j, T)$. For this scenario, let $Pr\{k\}$ be the probability that k indexes in $\mathcal{I}_S$ are found by the index finding attack. Suppose that N_T is the total number of vehicles passed the socialspot, N_V is the number of vehicles observed by adversary for the given time period T, and N_A is the number of chosen indexes in $\mathcal{I}_S$. The probability $Pr\{k\}$ can be represented as follow distribution:

$$Pr\{X = k\} = \frac{\binom{N_A}{k}\binom{N_T - N_A}{N_V - k}}{\binom{N_T}{N_V}}, \quad k \geq 0$$

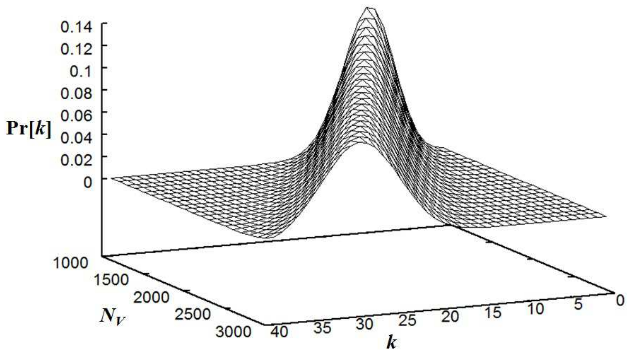


Figure 7: Index finding probability distribution for chosen index set by $\mathcal{A}$.

Figure 7 shows such index finding probability distribution by $\mathcal{A}$ assuming N_T is 10,000 and N_A is 1% of N_T for evaluation[2]. From this result, we can figure out that the index finding probability decreases as the number of vehicles N_V passing through a socialspot increases. Therefore, we can conclude that putting a special area where many vehicles visit in city road environments as a socialspot is helpful for privacy preservation for secure message delivery in VDTNs.

In addition, we surveyed traffic statistics reports for urban principal roads and intersections of Busan Metropolitan City, South Korea[3] to estimate the probability in a real road vehicle traffic environment. From the reports, we first categorized observation points into four cases to show apparent situation depending on the number of vehicles which the highest and the lowest traffics per hour (N_T) are approximately 10,000 and 3,500 vehicles, respectively.

- Type I : For the highest traffic, the number of service requesting vehicles N_V (i.e., observed vehicles by the adversary) is a higher case (Type I-1) and a lower case (Type I-2), respectively[4].

[2] The largest number of compromised vehicles was assumed with 1% in [Huang et al. 2011].

[3] `http://www.busan.go.kr/05field/0508traffic/04_02_01_01.jsp`

[4] We assumed below 20% and over 50% of N_T as a higher case and a lower case, respectively

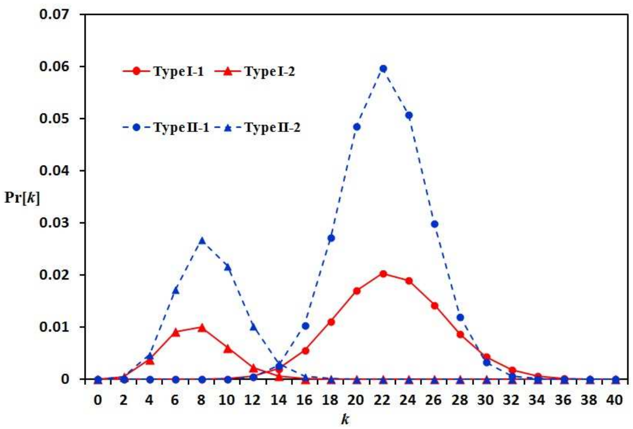


Figure 8: Index finding probability for four types of observation scenarios.

– Type II : For the lowest traffic, the number of service requesting vehicles is a higher case (Type II-1) and a lower case (Type II-2), respectively.

As shown in the Figure 8, the higher vehicle traffic cases show the lower index finding probability. On the other hand, Type II-1 case, which the number of passing vehicles at a socialspot is small but relatively large portion of vehicles request the message retrieving service, faces with the highest index finding probability.

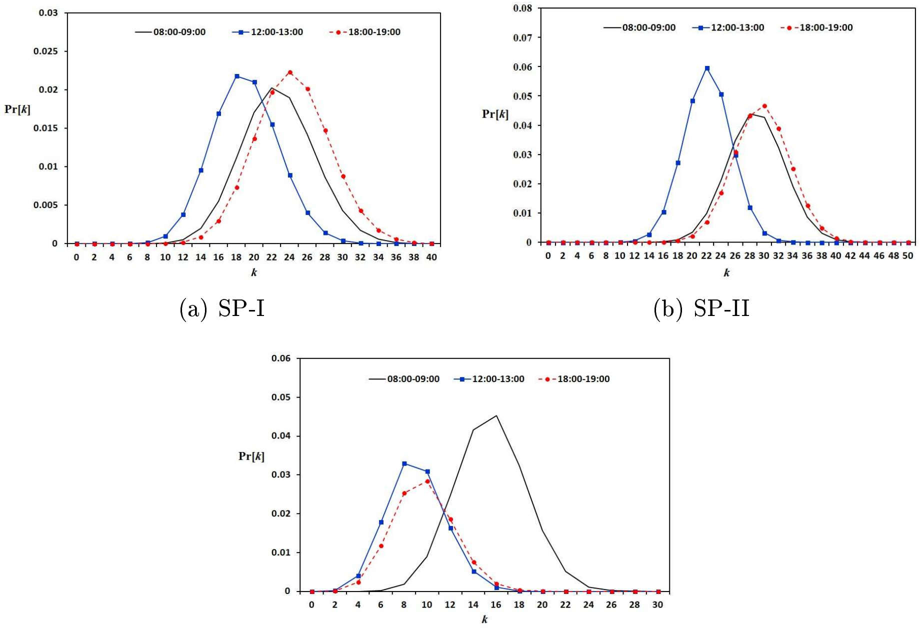
Furthermore, we selected three socialspot scenarios considering the characteristics of roads or driving patterns for some specific rush hour on each street around the socialspots as shown in Table 3.

Table 3: Traffic characteristics of each socialspot scenario.

	08:00-09:00		12:00-13:00		18:00-19:00	
	N_T	N_V	N_T	N_V	N_T	N_V
SP-I	10,411	2,196	8,722	1,828	10,006	2,360
SP-II	6,426	2,841	4,495	2,209	6,393	2,953
SP-III	4,205	1,491	3,820	833	4,601	889

– SP-I is an intersection of a subcenter of the city where the most amount of vehicles pass.

– SP-II is a street connecting a high-density residential area to center of the city.



(a) SP-I

(b) SP-II

(c) SP-III

Figure 9: Index finding probabilities for each socialspot scenario.

– SP-III is a downtown on which shopping malls and movie theaters are concentrated.

Figure 9 depicts the index finding probabilities for each socialspot scenario, respectively. Scenario SP-I which has the highest traffic shows lower probabilities rather than other scenarios and has similar probabilities for each time period. We can infer, in the case of SP-II, that morning rush hour for going to work and evening rush hour for coming home show relatively lower probabilities, and the probability of the evening time of SP-III is the lowest case because lots of vehicles are concentrated on a downtown area after work. Therefore, it is recommended to select a suitable socialspot for privacy-preserving message exchange depending on road characteristics and users driving patterns considering the results.

5 Conclusion

In this paper, we proposed a secure message delivery protocol with the help of socialspots in Vehicular Delay Tolerant Networks to provide anonymous message transmission and vehicle privacy preservation assuming a global passive adversary. To design a simplified protocol, we eliminated the pseudonym-based receiver vehicle identification accompanied with a complex pseudonymous key management. Instead, we made use of identity-hidden message indexing for a receiver vehicle to prevent vehicle's identity from being disclosed or linked by an adversary, and proof of knowledge for non-interactively shared key between sender and receiver to authenticate the receiver implicitly by a socialspot RSU. We demonstrated the efficiency of the proposed protocol by evaluating the message processing delay to show the reduced cryptographic overhead as comparing with a pseudonym-based approach. In addition, we showed that it is hard for an adversary to link a specific vehicle to a message index at a socialspot, and estimated the index finding probabilities for some specific socialspot characteristics considering city road environments.

Acknowledgements

This research was supported by Basic Science Research Program (No. 2012-0001331), and partially supported by Next-Generation Information Computing Development Program (No. 2011-0029927) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology.

References

[Allal and Boudjit 2013] Allal, S., and Boudjit, S.: "Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal"; Journal of Internet Services and Information Security, 3, 1/2 (2013), 20-36.

[Boneh and Franklin 2003] Boneh, D., and Franklin, M.: "Identity-based encryption from the Weil Pairing"; SIAM Journal of Computing, 32, 3 (2003), 586-615.

[Cha and Cheon 2003] Cha, J., and Cheon, J.: "Identity-based signature from gap Diffie-Hellman groups"; Proc. International Workshop on Practice and Theory in Public Key Cryptography(PKC 2003), LNCS 2567, Springer-Verlag (2003), 18-30.

[Dupont and Enge 2006] Dupont, R., and Enge, A.: "Provably secure non-interactive key distribution based on pairings"; Discrete Applied Mathematics, 154, 2 (2006), 270-276.

[Kim et al. 2008] Kim, H., Paik, J., Lee, B., and Lee, D.: "SARC: A street-based anonymous vehicular ad hoc routing protocol for city environment"; Proc. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (2008), 324-329.

[Huang et al. 2011] Huang, J.-H., Yeh, L.-Y., and Chien, H.-Y.: "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks"; IEEE Transactions on Vehicular Techonolgy, 60, 1 (2011), 248-262.

[Jeong et al. 2011] Jeong, J., Guo, S., Gu, Y., He, T., and Du, D. H. C.: "Trajectory-based data forwarding for light-traffic Vehicular Ad Hoc Networks"; IEEE Transaction on Parallel and Distributed Systems, 22, 5 (2011), 743-757.

[Jung et al. 2009] Jung, C., Sur, C., Park, Y., and Rhee, K.: "A robust and efficient anonymous authentication protocol in VANETs", Journal of Communications and Networks, 11, 2 (2009), 607-614.

[Kate et al. 2010] Kate, A., Zaverucha, G. M., and Goldberg, I.: "Pairing-based onion routing with improved forward secrecy"; Journal of ACM Transactions on Information and System Security (TISSEC), 13, 4 (2010), Article No. 29.

[Kenney 2011] Kenney, J.B: "Dedicated Short-Range Communications (DSRC) Standards in the United States"; Proceedigns of IEEE, 99, 7 (2011), 1162-1182.

[Lin et al. 2011] Lin, X., Lu, R., Liang, X., Shen X.: "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs"; Proc. IEEE INFOCOM (2011), 2147-2155.

[Lu et al. 2010a] Lu, R., Lin, X., Liang, X., and (Sherman) Shen, X.: "Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in VANET"; Proc. IEEE GLOBECOM (2010), 1-5.

[Lu et al. 2010b] Lu, R., Lin, X., Shen, X.: "SPRING: A social-based privacy-preserving packet forwarding protocol for Vehicular Delay Tolerant Networks"; Proc. IEEE INFOCOM (2010), 632-640.

[Lu et al. 2008] Lu, R., Lin, X., Zhu, H., Ho, P.-H., and Shen, X.: "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications"; Proc. IEEE INFOCOM (2008), 1229-1237.

[Nzouonta et al. 2009] Nzouonta, J., Rajgure, N., Wang, G., and Borcea, C.: "VANET routing on city roads using real-time vehicular traffic information"; IEEE Transactions on Vehicular Technology, 58, 7 (2009), 3609-3626.

[Park et al. 2010] Park, Y., Sur, C., Jung, C., and Rhee, K.: "An efficient anonymous authentication protocol for secure vehicular communications"; Journal of Information Science and Engineering, 26, 3 (2010), 1016-2364.

[Park et al. 2013] Park, Y., Sur, C., and Rhee, K.-H.: "A simplified privacy preserving message delivery protocol in VDTNs"; Proc. of ICT-EurAsia 2013, LNCS 7804 (2013), 416-425.

[PBC] The pairing-based cryptography library; [online] Available at : `http://crypto.stanford.edu/pbc`.

[Pereira et al. 2012] Pereira, P. R., Casaca, A., Rodrigues, J. J. P. C., Soares, V. N. G. J, Triay, J., and Cervello-Pastor, C.: "From delay-tolerant networks to vehicular delay-tolerant networks"; IEEE Communications Surveys & Tutorials, 14, 4 (2012), 1166-1182.

[Raya and Hubaux 2007] Raya, M., and Hubaux, J.-P.: "Securing vehicular ad hoc networks"; Journal of Computer Security, 15, 1 (2007), 39-68.

[Sakai et al. 2000] Sakai, R., Ohgishi, K., and Kasahara, M.: "Cryptosystems based on pairing"; Symposium on Cryptography and Information Security (2000).

[Smaldone et al. 2008] Smaldone, S., Han, L., Shankar, P., and Iftode, L.: "Roadspeak: enabling voice chat on roadways using vehicular social networks"; Proc. 1st Workshop on Social Network Systems (2008), 43-48.

[Sun et al. 2010] Sun, Y., Lu, R., Lin, X., Shen, X., and Su, J.: "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications"; IEEE Transactions on Vehicular Technology, 59, 7 (2010), 3589-3603.

[Wang and Li 2009] Wang, Y., and Li, F.: "Vehicular ad hoc networks"; Guide to Wireless Ad Hoc Networks, Computer Communications and Networks (2009), 503-525.

[Yang et al. 2010] Yang, Q., Lim, A., Ruan, X., and Qin, X.: "Location privacy protection in contention based forwarding for VANETs"; Proc. IEEE GLOBECOM (2010), 1-5.

[Zhang et al. 2007] Zhang, X., Neglia, G., Kurose, J., and Towsley, D.: "Performance modeling of epidemic routing"; Computer Networks, 51 (2007), 2867-2891.

[Zhao and Cao 2006] Zhao, J., Cao, G.: "VADD: Vehicle-assisted data delivery in Vehicular Ad Hoc Networks"; Proc. IEEE INFOCOM (2006), 1-12.