A Simplified Privacy Preserving Message Delivery Protocol in VDTNs

Youngho Park, Chul Sur, Kyung-Hyune Rhee

A Simplified Privacy Preserving Message Delivery Protocol in VDTNs*

Youngho Park, Chul Sur, and Kyung-Hyune Rhee

Department of IT Convergence and Application Engineering,
Pukyong National University, Busan, Republic of Korea.
{pyhoya, kahlil, khrhee}@pknu.ac.kr

Abstract. In Vehicular Ad Hoc Networks (VANETs), because of high mobility of vehicles and frequent change of road segments, an end-to-end communication path between moving vehicles may not exist unfortunately. As a promising solution to this challenge, for non-realtime constrained VANET applications, store-carry-forward paradigm is considered to deliver a message to a remote destination vehicle effectively through a socialspot in city road environments. So, the behavior of VANET can be modeled as Delay Tolerant Networks, and known as Vehicular Delay Tolerant Networks (VDTNs). Therefore, in this paper, we propose a secure message delivery protocol for protecting receiver-location privacy in socialspot-based VDTNs since location privacy is one of critical security requirements in VANETs. To design a simplified protocol, we eliminate the use of pseudonym-based vehicle identification accompanied with a complex pseudonymous key 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.

Keywords : VANET, VDTN, authentication, privacy preservation

1 Introduction

Vehicular Ad Hoc Networks (VANETs) to support the Intelligent Transportation Systems and Telematics have recently become one of the promising wireless networking research areas. This trend is due to Dedicated Short Range Communications (DSRC) [14] and the GPS-based navigation system incorporating with digital map. Typically, in VANETs, each vehicle equips with an on-board unit (OBU) communication device, which allows Vehicle-to-Vehicle (V2V) communication with other vehicles as well as Vehicle-to-Infrastructure (V2I) communication with a road-side unit (RSU). With these deployments, the VANET enables useful applications in our daily lives ranging from safety related to non-safety

* 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.

related, such as not only cooperative driving and probing vehicle data for better driving environment but also infotainment services by vehicular communications.

However, an end-to-end communication path between moving vehicles may not exist unfortunately because vehicles are constantly moving with frequently changing road segments which, in turn, makes network connectivity change. As a promising solution to this challenge, for non-realtime constrained VANET applications, store-carry-forward paradigm is considered to deliver a message to a multi-hop destination vehicle effectively by utilizing socialspot tactic [7] 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. Hence, we can utilize an RSU installed in the socialspot as a relay node for packet forwarding in an opportunistic way [7][8][6]. So, the behavior of a multi-hop VANET communication can be modeled as a Delay Tolerant Network known as Vehicular Delay Tolerant Networks (VDTNs), and packet forwarding protocols using store-carry-forward manner have been proposed [13][4].

As VANETs have received a lot of attention, security issues, especially privacy of vehicles or drivers, have become one of the most concerns for the successful deployment of VANET. In the same vein, socialspot-based VDTN applications must protect vehicle's privacy even though the locations of socialspots for message dissemination are known. 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

In order to protect receiver-location privacy in VDTNs, Lu et al. proposed socialspot-tactic privacy-preserving data forwarding protocols in [7] and [8], respectively. Those protocols are on the basis of pseudonym-based vehicle identification for anonymous message delivery and receiver authentication[1]. 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 pseudonyms pre-loaded, and all vehicles must know receiver vehicle's pseudonym to send a message to the receiver. What is worse, the protocol of [7] does not provide message source authentication so this protocol cannot guarantee the non-repudiation if a malicious vehicle sends a bogus message.

On the other hand, the authors [8] 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 vehicle to perform a complex mutual authentication

[1] When we say sender and receiver, they are end-to-end message source and destination vehicle in this paper, respectively.

process with RSU at the socialspot due to the much time consuming operation of group signature scheme.

1.2 Contribution and Organization

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 authentication process of a receiver vehicle to a socialspot RSU by eliminating the use of pseudonym-set. The contributions of this paper are summarized as follows.

- Instead of putting vehicles' pseudo-ID to identify a receiver vehicle in anonymous manner, we introduce an identity-hidden message indexing in order for a receiver vehicle to query the message bound for it to the socialspot RSU without revealing its identity.
- 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.
- To simplify the authentication process between a receiver vehicle and a socialspot RSU without presenting receiver's identity-related information, we make the receiver vehicle be implicitly authenticated to the RSU by proving knowledge of the shared secret key with the sender.

To design the proposed protocol, we make use of ID-based non-interactive key agreement scheme [12][3] (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. The remainder of this paper is organized as follows. In Section 2, we introduce our system model and security goals considered in this paper. We present the proposed protocol and provide security analysis in Section 3 and Section 4, respectively. Finally, we conclude in Section 5.

2 System Model

We consider a VDTN environment which consists of vehicles equipping with OBUs, RSUs installed in socialspots and Trusted Authority(TA) for security management as shown in Fig. 1, respectively.

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

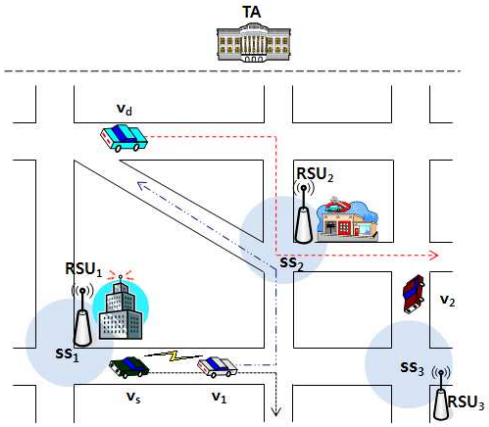

Fig. 1. System model for socialspot-based VDTN.

– 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 to deliver 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.

– Direct carry and forward : If the sender vehicle passes the socialspot, the sender will carry the message and then forward it when it arrives on the socialspot.
– V2V forward and carry : Some vehicles driving toward the socialspot will cooperate for store-carry-forward message delivery when the sender vehicle does not pass the socialspot.

As an example scenario, suppose that v_s wants to send a message msg to v_d which will visit socialspot ss_2 later in Fig. 1.

1. At time t_1, v_s asks v_1 which drives toward the ss_2 for forwarding the msg.
2. v_1 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

The proposed protocol consists of *setup*, *message constitution*, *message forwarding*, and *message retrieving* phases. Table 1 shows the notations and descriptions used in the proposed protocol.

Table 1. Notations and descriptions.

notation	description
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

3.1 Setup

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the bilinear map groups with a prime order q, and P be a generator of $\mathbb{G}_1$ [1], respectively. In the setup phase, the TA configures system parameters for bilinear map and issues ID-based private keys to the registered RSUs and vehicles as following steps.

1. TA sets a random number $s \in \mathbb{Z}_q^*$ as its master secret key, computes $P_0 = sP$, and configures public system parameters $param$=$\{\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, P_0, H_1, H_2\}$, where $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map, $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ are cryptographic hash functions, respectively.
2. 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 $SK_j = sH_1(ss_j)$ 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 following steps to make a packed message.

1. v_s chooses a random number $r \in \mathbb{Z}_q^*$ and computes $P_s = rH_1(v_s)$, $k_{sd} = \hat{e}(rSK_{v_s}, H_1(v_d))$, $k_{sj} = \hat{e}(rSK_{v_s}, H_1(ss_j))$, $w = H_2(k_{sd}|T)$, and $W = w^{-1}P$, where k_{sd} and k_{sj} are non-interactively shared keys with v_d and with RSU_j, respectively.
2. Then, v_s constitutes a packed message M to be forwarded to the destination socialspot ss_j as follows:
   $M = \{ss_j, I, P_s, W, C|\sigma, chk\}$
   - $I = h(v_d, ss_j, T)$
   - $C = Enc_{k_{sd}}(v_s|v_d|T|msg)$
   - $\sigma = Sig_{SK_{v_s}}(v_s|v_d|T|msg)$
   - $chk = MAC_{k_{sj}}(ss_j, I, P_s, W, C|\sigma)$

   where σ is sender v_s's ID-based signature of [2], and chk is a message authentication code for integrity check by RSU_j.

In step 2, the identity-hidden message index I implies the meaning of a receiver vehicle v_d at a socialspot ss_j, and will be used for a receiver vehicle to query a message for it in the message retrieving phase.

3.3 Message Forwarding

Once the message M is packed, M can be delivered to a destination socialspot ss_j by using the forwarding strategy described in Section 2. At this phase, we assume a packet forwarding protocol with store-carry-forward manner, such as VADD [13] and TBD [4]. 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.

When the message M ultimately reaches the RSU_j at ss_j, RSU_j first computes shared key of v_s as $k_{sj} = \hat{e}(P_s, SK_{ss_j})$ from P_s in M. Then, RSU_j verifies $chk = MAC_{k_{sj}}(ss_j, I, P_s, W, C|\sigma)$ under the key k_{sj}. If chk is valid, RSU_j stores $\{I, P_s, W, C|\sigma\}$ while a receiver vehicle related to the message index I requests the message as passing by it.

3.4 Message Retrieving

Fig. 2 shows the message retrieving protocol of a receiver vehicle at a socialspot. 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 as follows.

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.

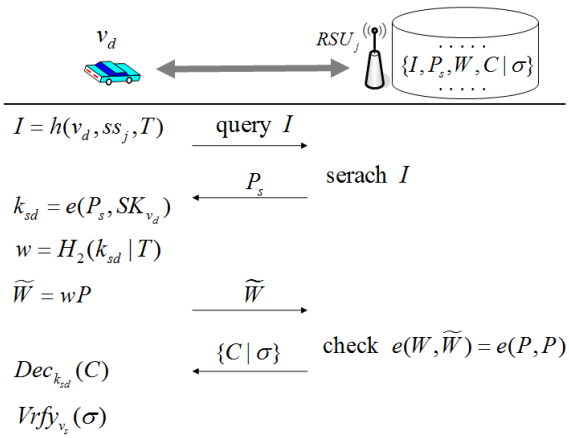

Fig. 2. Message retrieving protocol of a receiver vehicle at a socialspot.

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 verifies $\hat{e}(W, \widetilde{W}) = \hat{e}(P, P)$ to check 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 $\{v_s|v_d|T|msg\}$ by computing $Dec_{k_{sd}}(C)$, and finally completes the message retrieving protocol after verifying the signature σ as $Vrf_{v_s}(\sigma)$.

4 Analysis

In this section, we discuss the security of the proposed protocol. 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.

4.1 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 [3], 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 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. [5] presented that they could construct an onion routing for anonymity network on the basis of non-interactive key agreement scheme. If we encrypt the packed message M again under key k_{sj} instead of $MAC_{k_{sj}}$ in Message Constitution phase, the path $v_s \rightarrow ... \rightarrow RSU_j \rightarrow v_d$ can be regarded as an onion path based on Kate et al.'s observation.

4.2 Authentication

In order to obtain a message temporarily stored in a 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 $\hat{e}(rSK_{v_s}, H_1(v_d))$ generated by v_s and $\hat{e}(P_s, SK_{v_d})$ by v_d can be proven as $\hat{e}(rSK_{v_s}, H_1(v_d)) = \hat{e}(rH_1(v_s), sH_1(v_d)) = \hat{e}(P_s, SK_{v_d})$.

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 $T' \neq T$, 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 $\mathcal{I}_S$ from arbitrarily chosen vehicles identities $\mathcal{V}_A = \{v_1, ..., v_m\}$ by $\mathcal{A}$ for a given time period T, and check if an $I \in \mathcal{I}_S$ 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 among N_V vehicles passing through the socialspot ss_j for the given time period T are found by the index matching attack. Suppose that N_R is total number of registered vehicles and N_C is the number of elements in $\mathcal{I}_S$. The probability $Pr\{k\}$ can be represented as follow distribution:

$$Pr\{X = k\} = \frac{\binom{N_C}{k}\binom{N_R - N_C}{N_V - k}}{\binom{N_R}{N_V}}, \quad k \geq 1$$

As a result, the probability that a target vehicle v_d can be linked to $\mathcal{I}_S$ is $Pr\{k = 1\}$. Fig. 3 shows such link probability under chosen message index matching attack by $\mathcal{A}$ assuming $N_R = 10,000$ for evaluation. From this result, we can figure out that the link 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 frequently visit in city road environments as a socialspot is helpful for privacy preservation for secure message delivery in VDTNs.

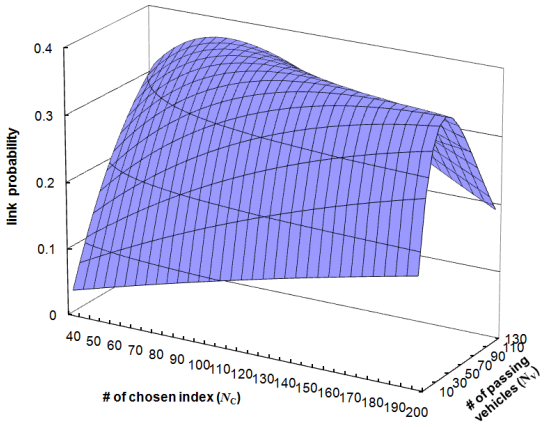

Fig. 3. Link probability for $k = 1$ under chosen message index matching by $\mathcal{A}$.

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 vehicles 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.

In addition, we showed that it is infeasible for an adversary to link a specific vehicle to a message index at a socialspot.

References

1. D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3, pp.586–615, 2003.
2. J. Cha, and J. Cheon, "Identity-based signature from gap Diffie-Hellman groups," Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography(PKC 2003), LNCS 2567, Springer-Verlag, pp.18–30, 2003.
3. R. Dupont and A. Enge, "Provably secure non-interactive key distribution based on pairings," Discrete Applied Mathematics, vol. 154, no. 2, pp.270–276, 2006.
4. J. Jeong, S. Guo, Y. Gu, T. He, and D. H. C. Du, "Trajectory-based data forwarding for light-traffic Vehicular Ad Hoc Networks," IEEE Transaction on Parallel and Distributed Systems, vol. 22, no. 5, pp.743–757, 2011.
5. A. Kate, G. M. Zaverucha, and I. Goldberg, "Pairing-based onion routing with improved forward secrecy," Journal of ACM Transactions on Information and System Security (TISSEC), vol. 13 no. 4, Article No. 29, ACM, 2010.
6. X. Lin, R. Lu, X. Liang, X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," Proceedings of the IEEE INFOCOM, pp.2147–2155, 2011.
7. R. Lu, X. Lin. X. Liang, and X. (Sherman) Shen, "Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in VANET," Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), pp.1–5, 2010.
8. R. Lu, X. Lin, X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for Vehicular Delay Tolerant Networks," Proceedings of the IEEE INFOCOM, pp.632–640, 2010.
9. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," Proceedings of the IEEE INFOCOM, pp.1229–1237, 2008.
10. J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," IEEE Transactions on Vehicular Technology, vol. 58, no. 7, pp.3609–3626, 2009.
11. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp.39–68, 2007.
12. R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," Symposium on Cryptography and Information Security (SCIS 2000), 2000.
13. J. Zhao, G. Cao, "VADD: Vehicle-assisted data delivery in Vehicular Ad Hoc Networks," Proceedings of the IEEE INFOCOM, pp.1–12, 2006.
14. "Dedicated Short Range Communications (DSRC)," [Onlilne] Available: http://www.leearmstrong.com/dsrc/dsrchomeset.htm.