Covert Communication based Privacy Preservation in Mobile Vehicular Networks

Rasheed Hussain*, Donghyun Kim†, Alade O. Tokuta†, Hayk M. Melikyan†. and Heekuck Oh‡
* Department of Computer Science, Innopolis University, Kazan, Russia
E-mail: rasheed1984@gmail.com
† Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA
E-mail: {donghyun.kim, gmelikian, atokuta}@nccu.edu
‡ Department of Computer Science and Engineering, Hanyang University, ERICA Campus, South Korea
E-mail: hkoh@hanyang.ac.kr

***Abstract*—Due to the dire consequences of privacy abuse in vehicular ad hoc network (VANET), a number of mechanisms have been put forth to conditionally preserve the user and location privacy. To date, multiple pseudonymous approach is regarded as one of the best effective solutions where every node uses multiple temporary pseudonyms. However, recently it has been found out that even multiple pseudonyms could be linked to each other and to a single node thereby jeopardizing the privacy. Therefore in this paper, we propose a novel identity exchange-based approach to preserve user privacy in VANET where a node exchanges its pseudonyms with the neighbors and uses both its own and neighbors' pseudonym randomly to preserve privacy. Additionally the revocation of the immediate user of the pseudonym is made possible through an efficient revocation mechanism. Moreover the pseudonym exchange is realized through covert communication where a side channel is used to establish a covert communication path between the exchanging nodes, based on the scheduled beacons. Our proposed scheme is secure, robust, and it preserves privacy through the existing beacon infrastructure.**

***Keywords*—VANET, Covert Communication, Pseudonyms, Beacons, Conditional Privacy.**

I. Introduction and Related Work

Today world leading automobile companies are optimizing their high-end vehicles by adding consumer comfort services to their products such as smart parking, driving assistance, in-car infotainment system, and so forth. Nonetheless, cross-platform optimization and integration is essential to globally adapt the intelligent transportation system (ITS) technology. ITS is realized through vehicular ad hoc network (VANET) where vehicles communicate with each other (V2V) and with the infrastructure (V2I), regardless of their brands and other characteristics. VANET is based on IEEE 802.11p standard also known as dedicated short range communication DSRC standard [1]. Among many other messages related to VANET, the standard SAE J2735 mandates a frequent cooperative awareness message (CAM) also referred to as beacon that contains the current mobility statistics including current speed, position, acceleration, and vehicle control information.

Among other challenges, security and privacy have the pivotal role in the future of VANET because it directly affects the end users and their privacy rights. Consumers would never adopt a technology at the expense of their privacy. Therefore the research community has addressed the security and privacy challenges in VANET in detail [2]–[5]. Solutions to privacy problems in VANET include mix zones [6], silent periods [2], identityless mechanism [3], and multiple pseudonymous mechanism [5]. In mix zones, there is a designated area where the nodes change their security keys. Similarly in the silent period, the nodes stop communicating with each other and change their security keys and temporary identities, if any. These mechanisms have adverse effect on the VANET applications. Among other techniques, multiple pseudonyms are regarded as one of the best solutions to preserve privacy [5]. However, it has been found out that statistically multiple pseudonyms can still be linked to each other and movement profiles can be constructed [7]. Therefore Eckhoff et al. [4] proposed an identity diffusion method which let the nodes to swap their identities and use the identities based on predefined time windows and they used predefined time slots. However, the degree of anonymity still depends on the length of the time window. Therefore another effective, robust, and efficient mechanism is essential to conditionally preserve the user privacy. An abstract idea of pseudonym exchange is outlined in [8] without firm details. In this paper we propose a novel pseudonym exchange based approach to preserve privacy where the nodes exchange their pseudonyms with their neighbors. They have choice to either use their own pseudonyms or the exchanged pseudonyms during communication. For pseudonym exchange among neighbors, we leverage the scheduled beacons-based communication and a covert side-channel where beacon messages are deliberately corrupted in a way that the phenomenon statistically mimics the natural corruption of the packets. Based on shared secret between the communicating parties, they can extract the pseudonym from the corrupted packet. The reason for using covert communication is to keep the adversary at the bay from figuring out that the pseudonym exchange took place.

Rivest for the first time proposed a covert, non-cryptographic approach to provide confidentiality in communication through winnowing and chaffing [9]. With the real message, some chaff (redundant immaterial) is also included to provide indistinguishability and confidentiality at the same time. The real intended user can get the original message because it holds the secret key. Recently, anonymous and deniable communication mechanism named DenaLi was proposed by Narain et al. [10] where they considered point-to-point networking for anonymous communication. They use a covert

channel based approach for such communication where they send the secret messages in the corrupted frames. The intended users can extract the secret messages from the corrupted frames with the help of pre-shared secrets. However, in DenaLi the authors consider point-to-point networking and they provide complete deniability which is questionable in our scenario. In case of VANET, providing conditional deniability and conditional privacy is a challenge that has not been addressed by DenaLi. Another covert communication based misbehavior reporting scheme was proposed by Fuentes et al. [11] where they use two information hiding techniques, subliminal channel and steganography. They also embed these approaches to the beacon messages; however, their scheme does not provide privacy and is prone to profilation and other privacy abuses. Moreover it has also been found out that the errors in the frames are not bit-wise, but in the form of chunks and the probability of errors varies with the bit positions in the frame. The farther bits in the frame are more prone to errors [12]. The contribution of this paper are listed below:

(a) We propose a novel pseudonym exchange-based privacy preservation mechanism for vehicular networks where vehicles have choice to either use their own pseudonyms or use others' to increase their conditional anonymity.
(b) We use a new beacons-based covert communication to exchange pseudonyms among the nodes in a secure, conditionally deniable, and confidential way.
(c) We also propose a robust revocation mechanism to carry out the revocation process in case of complex pseudonym exchange.

The rest of the paper is organized as follows: in Section II we outline our proposed scheme followed by quantitative evaluation in section III. In section IV, we give the concluding remarks as well as future directions.

II. Proposed Covert Privacy Preserving Scheme

A. System Players and Network Model

The proposed network model is based on signature VANET that consists of management and users. The management consists of the department of motor vehicles (DMV), a trusted entity that is responsible for the registration and initialization, revocation authorities (RAs), certification authorities (CAs), and roadside units (RSUs). Users are the vehicles equipped with onboard units (OBU) and tamper resistant module (TRM). OBUs are compliant with the DSRC standard SAE J2735 and IEEE 1616[1] that defines the sensorial data representation for the beacon construction. Without loss of generality, we only consider beacons-based communication for pseudonyms exchange. The network model of our proposed scheme is illustrated in Fig. 1. The requirements of our system are *Communication anonymity, Indistinguishability, Offset calculation, Profilation protection, Undetectability, Unlinkability,* and *Robustness*. The goal of our proposed scheme is to fulfill the aforementioned requirements.

B. Preliminaries and Initializations

Every vehicle carries a pool of pseudonyms issued by the DMV at the time of registration. For revocation purpose, the

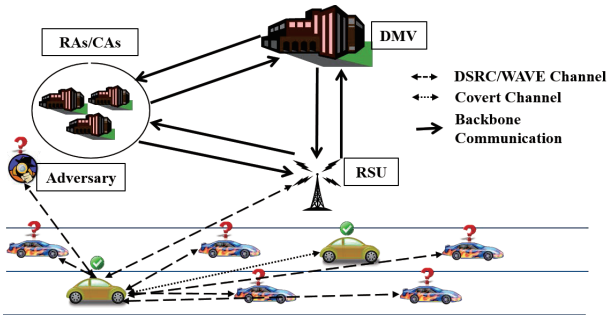


Fig. 1: Proposed Network Model.

secret keys are encrypted and stored in RAs. These secret keys include K_{psu}, a symmetric key used for pseudonym generation and K_{OBU}, vehicle's individual secret key. To store these keys in the RAs, we use ElGamal encryption algorithm over elliptic curve cryptography (ECC) due to its proven security. Let $\mathbb{G}$ be a cyclic group of prime order q where $\mathbb{G}$ is generated by a generator G. First of all DMV chooses a random number $k \in \mathbb{Z}^*$ as its private key and computes $PK^+ = kG$ as its public key. In order to distribute the shares of the secret keys among the RAs, DMV employes threshold based secret share scheme and divides k into l parts where l is the number of RAs, each RA_i holds a share k_i and $k_i \in (k_1, k_2, k_3, ..., k_l)$. We assume that any existing threshold based secret sharing scheme can be used for this purpose [13].

C. TRM Initialization

After confirming the credentials of the vehicle and its owner, DMV initializes TRM and saves the system parameters in the TRM including $(\mathbb{G}, q, G, PK^+, c_{init}, a_V)$. Additionally DMV also preloads TRM with K_{OBU} and K_{psu}.

D. Pseudonym Generation

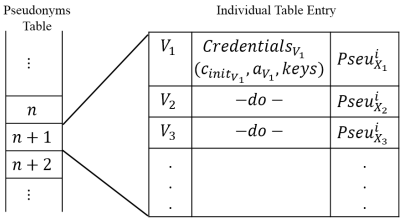
DMV generates a large pool of pseudonyms for every vehicle, let say n number of pseudonyms. It is worth noting that the pseudonyms are made secretly traceable to enable the revocation by the RAs when needed. DMV puts a trapdoor (VIN) in the pseudonym. For pseudonym generation, DMV takes vehicle V's secret initial value c_{init} and increments it by vehicle V's incrementing factor a_v. Thus the individual pseudonym is a package of the following values:

$$Psue_X^i = \{(\epsilon)_{K_{psu}} || (\epsilon \oplus VIN)_{K_{OBU}} || n_i || Validity\}_{K_{DMV}^-},$$

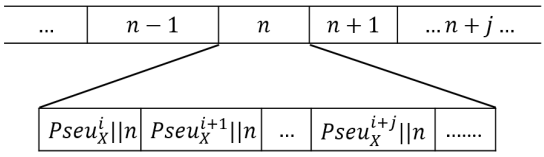
where $\epsilon = c_{init} + n_i a_v$, n_i is the current count of generated pseudonym which may not necessarily be linear (in order to randomize the pseudonym generation), and VIN is the vehicular identification number which according to the ISO 3780, consists of 17 alphanumeric elements[2]. DMV also maintains a pseudonyms database where pseudonyms are indexed with the value of n. When the pseudonym generation phase is completed, DMV stores the pseudonyms along with anonymous certificates in vehicle's TRM. The anonymous certificates are used for the pseudonym exchange phase during the covert communication. Moreover DMV also sends the anonymous

[1]Institute of Electrical and Electronics Engineers (IEEE), "Motor Vehicle Event Data Recorders (MVE-DRs)," IEEE Std 1616, 2005.

[2]International Standards Organization (ISO), ISO 3780 Road Vehicles-World Manufacturer Identifier (WMI) Code, 2009.



(a) Pseudonym Table at DMV



(b) Pseudonym Table at RAs

Fig. 2: Pseudonym History tables at DMV and RAs

pseudonyms and certificates to RAs as well. We do not give the exact details of the anonymous certificate and assume that the existing secure and privacy-aware anonymous certificates such as outlined in [14], [15] can be used in our proposed scheme. TRM encrypts K_{psu} and K_{OBU}, 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:

$$c_1 = dG \text{ and } c_2 = (K_{psu}||K_{OBU}) \oplus H(dPK^{+}).$$

d is a random nonce, a parameter selected by the TRM for ElGamal encryption. TRM sends the ciphertext (c_1, c_2) to RAs. However RAs can only decrypt the ciphertext, i.e. keys K_{psu} and K_{OBU} when there is a proper warrant for revocation. In such case, RAs collude to construct k from individual shares k_i.

Since DMV is a trusted party, therefore DMV maintains a database where it saves the issued credentials to the vehicles (VIN, c_{init}, a_v) and whose TRHs are initialized by DMV. Pseudonyms are maintained by DMV and indexed with the value of n as shown in Fig. 2a. Moreover RAs also anonymously maintain the history of issued pseudonyms as shown in Fig. 2b.

E. Message(Beacon) Format

In the proposed scheme, we deal with the corrupted beacon messages. The generic frame format of the IEEE 802.11p is given below:

$$F = (Header(30)\|Payload(0-2312)\|CRC(FCS-4))$$

At the end of the MAC frame, there is a 4 byte frame control sequence (FCS) field that contains the CRC value which determines the integrity of the frame. If the FCS value is not sound, the message is dropped. The same concept is leveraged to deliberately corrupt the frame by appending a random 4 bytes number. The covert beacon format is given below:

$$CB_X = \{B_{ID}||L||Pseu^i_X||Pl(PECB)||HMAC(Pl, K_{temp}) \\ Cert_{anony}||Sec.Param||(intent)\}_{K_{geolock}}$$

The above message is broadcasted by the node X that includes the pseudonym $Pseu^i_X$. It is worth noting that during the course of identity exchange, same pseudonym must be used, the exchange will fail, otherwise. In compliance with DRSC standard SAE J2735, beacons are sequentially numbered, represented by B_{ID}. We use that characteristic to calculate the offset where the pseudonym will be placed in the message during the exchange procedure. Pl represents the normal beacon payload. We refer to a part of this data as pseudonym exchange control bytes (PECB). PECB consists of size of the pseudonym followed by the actual pseudonym that needs to be exchanged. Moreover it also includes the $Offset$, the address (bytes) where the pseudonym will be placed. Note that the offset information is known to both the parties. The L field indicates the length of the secret contents of the message, i.e. exchanging pseudonym. The length of the pseudonym is fixed and is known to the communicating parties beforehand, however; in order to make it indistinguishable for the adversaries to find out covert communication, some salt is added to the pseudonym. The receivers can then separate the salt in order to receive the original pseudonym. We also use location-based encryption (geolock-based encryption [16]) to secure the beacon message from the outsiders and limit the insider adversaries. The contents of these parameters are given below:

$$PECB = (Size, Offset, Psu^e_V)$$
$$Offset = f(B_{ID}, K_{geolock_t})$$
$$f() = HMAC((B_{ID}, K_{geolock}), K_{temp})$$

In order to randomize the pseudonym exchange, the offset is randomized as well to increase the covertness of the message. Statistically the errors occur in wireless frames in the form of chunks and at the later bytes [12]. The offset is calculated through one public value and another group secret value, i.e. beacon ID and the geolock key, respectively and a keyed HMAC is calculated with the session key to calculate the offset. The receiver of the covert message calculates this offset to extract the exchanged pseudonym from the covert message. It is also to be noted that once the FCS field is corrupted in the frame, then there is no way for the receiver to check the integrity of the message, therefore we include the keyed HMAC of the payload contents along with the payload to check for the integrity of the contents.

F. Exchange Initiation

Due to the broadcast nature of the beacons in VANET, it is more challenging to establish a covert channel than unicast communication. Therefore we include an *intent* flag in the beacon that represents the interest of the nodes to exchange pseudonym. If the intent flag is ON in the received beacon message, then the sender is willing to change its pseudonym. However this flag can have adverse effect on the privacy of the exchanging parties as well, because the adversary can know that after the intent flag is ON, there will be a pseudonym exchange. Therefore we need to create some false alarms and redundant flag initiation as well. In the response of the intent flag, the other party also responds with the intent flag ON and then they initiate the session key establishment through covert channel.

G. Pseudonym Exchange

To exchange a valid pseudonym, the initiator turns ON the intent flag in the next scheduled beacon. At the receiver end, the interested vehicles also flip the flag to show their interest for pseudonym exchange. Nonetheless, false alarms exist to keep the adversaries at the bay from distinguishing between normal traffic and the pseudonym exchange traffic. When both the parties agree on exchanging their pseudonyms, they establish a session key K_{temp}. We assume that any existing efficient session key establishment protocol can be used.

Once the session key is established, the initiator takes the pseudonym, adds some salt to it and then calculates the $offset$ in the next scheduled beacon. The initiator puts the pseudonym at the location referred to by the calculated offset. The initiator also calculates the hash value of the payload with the session key. Then the CRC field of the outgoing frame is corrupted/changed. The intended receiver upon receiving such message first checks the CRC, if it is not sound then checks for the pseudonym that was used in the agreement phase. Upon success, the receiver calculates the offset and extracts the pseudonym. If the pseudonym is valid, then the receiver repeats the same process to send its own pseudonym to the exchanging party. Afterwards, both the parties send the exchange report to the revocation authorities.

H. Exchange Reporting

After the successful or unsuccessful exchange of pseudonyms, both the parties report the result of the exchange to the authorities which will aid the authorities in the revocation process afterwards. It is to be noted that sending exchange report to the authorities makes logical sense because if any node exchanges its pseudonym then the node does not take a risk to let the other party misuse the pseudonym and the revocation authorities may trace it back to the owner. Therefore, the exchanging nodes report their pseudonym exchange. There are two types of reports that the nodes may send to the RAs. Incomplete Exchange Report (IER) is sent to RAs by the initiator if it sends its own pseudonym to its exchanging counterpart but the responder does not send its pseudonym back for any reason. And Complete Exchange Report (CER) is sent to RAs when the initiator and responder both successfully exchange their pseudonyms. The authorities maintain a Pseudonym Exchange Record (PER) which is maintained according to the time of exchange. The overall exchange process from both receiver's and the sender's standpoint is explained in Algorithm 1 and Algorithm 2.

I. Revocation Mechanism

In order to initiate the revocation process, after getting a warrant, RAs look into the concerned message to check for the pseudonym that has been used. RAs search the pseudonym related to value n and then search the exchange record (PER) to figure out whether the pseudonym was used by its original owner or exchanged with another user. PER will let the RAs know the exact target of the revocation. After searching PER based on recent time value, RAs collude and construct k from individual k_i related to the pseudonym in question and the session leader decrypts the keys from cipher text $c = \{c_1, c_2\}$

Algorithm 1 PseuRecv

Require: $(B_i, Psu^i_X, K_{temp}\ Established)$
Ensure: $Status_{(Partial\ Exchange)} = TRUE/FALSE$
1: Assumption: The session with K_{temp} is established with $Pseu^i_{V_x} \longleftrightarrow Pseu^j_{V_y}$
2: Beacon received
3: Check CRC
4: **if** $(CRC(Frame) == CRC_{received})$ **then**
5: Pass the beacon to the application buffer
6: **else** Pass pseudonym to the covert module
7: **if**$HMAC(Pl, K_{temp}) == HMAC_{received}$ **then**
8: $Offset = f()$ ▷ Calculate Offset by taking the hash of B_{ID} and $K_{geolock}$
9: **for** $i = Offset$ to $i \leq Sizeof(Pseu) \times 8$ and $i = i + 1$ **do**
10: $Buffer \longleftarrow Pseu$
11: **end for**
12: Retrieve Pseudonym
13: **else** Discard
14: **end if**
15: Check whether received pseudonym is valid and benign
16: **if** valid and sound **then**
17: Initiate Report (either IER or CER)
18: **else** Report pseudonym to the authorities
19: **end if**
20: **end if**
21: **return** $Status_{(Partial\ Exchange)} = TRUE/FALSE$

Algorithm 2 PseuRecv

Require: $(CB_i, Pseu^i_{V_x}, K_{temp}\ Established)$
Ensure: $Status_{(Partial\ Exchange)} = TRUE/FALSE$
1: Assumption: The session with K_{temp} is established with $Pseu^i_{V_x} \longleftrightarrow Pseu^j_{V_y}$
2: $CRC = rnd(Sizeof(CRC)) \longleftarrow CRC(Frame)$
3: $Offset \longleftarrow f((B_{ID}||Geolock), K_{temp})$
4: $Address(Offset) \longleftarrow Pseu^i_{V_x}$
5: $Output\ Buffer \longleftarrow Pseu^i_{V_x}$
6: **if** $(Buffer_{received} = Pseu^j_{V_y})$ **then** Prepare Exchange Report
7: **else if** Pseudonym not received from other party
8: $wait()$ until received and then report
9: **else** Report partial exchange
10: **end if**
11: **return** $Status_{(Exchange)} = TRUE/FALSE$

as follows:

$$Pseu^i_X = c_2 \oplus H(kc_1) = (K_{psu}||K_{OBU}) \oplus H(dPK^+) \oplus H(dkPK^+)$$

When RAs decrypt the keys K_{psu} and K_{OBU}, then they have to decrypt $(\epsilon)_{K_{psu}}$ and extract VIN from the pseudonym.

III. Quantitative Evaluation

In this section we quantitatively evaluate our proposed scheme.

Algorithm 3 RevoPseu ($(Psu^i_X)_{[t_x,t_y]}, i \in [1,n], j \in V$)

1: Extract the pseudonyms in question in time interval $[t_x, t_y]$
2: **for** $k = t_{cur}$ to $k = 1$ and *decrement time* **do**
3: Search for exchanged pseudonyms
4: **if** Found **then** Confirm the level of exchange and extract the sender of the pseudonym
5: **else** Break
6: **end for**
7: Search for concerned pseudonym in the pseudonym table
8: Construct k from k_i
9: Decrypt K_{psu} and K_{OBU}
10: Extract VIN_{V_j} from $(\epsilon)_{K_i}||(\epsilon \oplus VIN)_{K_{OBU}}$
11: **return** $VIN_{V_j} \leftarrow Pseu^i_X$

A. Security and Conditional Privacy Preservation

The goal of our proposed is to preserve conditional privacy through the use of exchanged pseudonyms. Moreover, the exchange process is also confidential so that the attackers cannot link the pseudonym exchange to the communicating parties. Since the communication is based on a covert channel, any node that does not have the session key K_{temp}, cannot know the pseudonym exchange process, at least with a negligible probability. The beacon message is secure from the outsiders since it is encrypted with $K_{geolock}$ and it is also secure from the insiders since the payload is encrypted with K_{temp} which is only known to the communicating parties. When a beacon with wrong CRC is broadcasted, then the receivers except the intended receiver drop it immediately, only the intended receiver with the shared secret can extract pseudonym from it.

Theorem III.1. *The proposed scheme increases the privacy of the user through exchanged pseudonyms.*

Proof: Continuing from the previous discussion, let suppose at time t_i a node V_1 uses its pseudonym $Pseu^i_{V_1}$ at location loc_i and the same pseudonym was used by another vehicle V_2 at loc_j at t_{i-j}. Then if the pseudonym exchanging vehicles V_1 and V_2 are at a safe distance from each other, then the relation $\triangle loc > d_{\triangle t}$ where d is the distance travelled by the vehicle. In other words, if the adversary has these messages from both the nodes, it will be hard to figure out who sent these messages, and whether it was generated by single or more than one vehicles. ■

Theorem III.2. *Revocation is possible at any level of the pseudonym exchange and the VIN of the immediate user of the pseudonym is revoked.*

Proof: Revocation is of prime concern in conditional privacy. The revocation is made sure according to Algorithm 3. At the end of the following algorithm, the VIN of the vehicle who sent the message (no matter which pseudonym was used) will be revoked provided that all the prerequisites for revocation are met. ■

The effect of keys compromise will be catastrophic for the covert communication especially K_{temp}. The compromise of K_{temp} will let the adversary know the pseudonym exchanging parties and will be able to profile them. Moreover confidentiality and timeliness are provided by $K_{geolock}$.

B. Computation and Communication Overhead

Since our proposed scheme leverages only beacon messages to exchange pseudonyms, therefore there is no additional communication overhead. The communication overhead can be considered as the frequency of beacons which is the adapted beacon frequency in our case. In other words, our prosposed scheme does not incur any additional communication overhead, because the information is sent through beacons. The revocation can be performed in two ways, either directly or through pseudonyms exchange reports. In the case of direct, the overhead incurred by our scheme, denoted by Rev_{direct} is given below:

$$Rev_{direct} = Cost(SearchTable_{pseu}\&PER) + Cost(ExtractK_{pseu}, K_{OBU}) + Cost(Symm.Decryption)$$
$$Rev_{direct} = 2T_\lambda + 2T_m + 2T_H + 2T_{sym-dec}$$

T_λ is the time incurred by the pseudonym search process ($Table_{pseu}$-pseudonym table and PER), T_m is the time required for point multiplication, T_H is the time required to calculate hash, and $T_{sym-dec}$ is the time required for symmetric decryption. If the pseudonym is used simultaneously, then first RAs point out the users who had the pseudonym. RAs need to examine all the current holders of the pseudonym in question that was used simultaneously. The revocation in such case consists of finding the nodes that possessed and used the pseudonym and then compare their $h_{K_{OBU}}(\cdot)$ values with the pseudonym in question. The revocation cost of the indirect revocation denoted by Rev_{indir} is given by:

$$Rev_{indir} = 2T_\lambda + 2\sum_{i=1}^{j}(T_{m_i} + T_{H_i} + T_{sym-dec_i}) + \sum_{i=1}^{j} T_{h_{i,k}}.$$

$T_{h_{i,k}}$ is the time required for keyed hash calculation and in case of indirect revocation, RAs have to examine j number of nodes. Zhang et al. found that T_m is equal to $0.78\ ms$ for a supersingular curve with embedding $k = 6$ over $\mathbb{F}_{3^{97}}$ [13]. Therefore the cost incurred can be written as:

$$Rev_{direct} = 1.56 + 2(T_\lambda + T_H + T_{sym-dec})$$
$$Rev_{indir} = 2T_\lambda + j \times 1.56\sum_{i=1}^{j}(T_{H_i} + T_{sym-dec_i}) + \sum_{i=1}^{j} T_{h_{i,k}}$$

C. Comparison with Known Schemes

To the best of our knowledge, [10] and [11] are the most relevant works to our scheme. Therefore we quantitatively compare our proposed scheme with DenaLi [10] and [11]. The comparison matrices are conditional privacy preservation, revocation, profilation, location confidentiality, and separate message infrastructure. The comparison is outlined in Table I. As it can be seen in the table that our proposed scheme preserves conditional privacy rather than fully deniable communication, which is questionable in real world. Moreover, since DenaLi [10] is based on unicast communication, it needs a separate message infrastructure to carry out the covert communication, whereas in our case we leverage the existing broadcast bandwidth used by the beacons. Additionally, our proposed scheme avoids profilation through geolock-based security mechanism thereby providing location security and confidentiality whereas DenaLi [10] and [11] do not. The revocation is not possible in DenaLi and [11] did not consider

TABLE I: Comparison with Known Solutions

Scheme	Separate Message Paradigm	Conditional Privacy	Profilation	Location Confidentiality against outsiders	Revocation Cost
DenaLi [10]	✓	✗	✓	✗	N/A
Fuentes et al. [11]	✗	✗	✓	✗	Not discussed
Our Scheme	✗	✓	✗	✓	$1.56 + 2(T_\lambda + T_H + T_{sym-dec})$

revocation. The requirements of our scheme are more challenging than DenaLi and [11], and from security and privacy perspective, our proposed scheme outperforms the formers.

D. Discussion

Dynamic beacon frequency is more favorable for the VANET applications than static frequency. Due to the wireless communication, there is always loss is beacon reception. Our main idea is to leverage that quota and insert some erroneous messages into the stream of beacons. The higher traffic density is more favorable for our covert communication for several reason: it will anonymize the exchange process and the covert communication will be difficult to distinguish. For single pseudonym exchange between two nodes, at least $(5 + y)$ messages must be exchanged where 5 is the minimum number of messages to be exchanged and y is the number of messages exchanged for the session key establishment.

IV. Conclusions

In this paper, we proposed a multiple pseudonymous covert communication-based mechanism to preserve conditional privacy in mobile VANET. The nodes have choice to either use their own pseudonyms or exchanged pseudonyms with the neighbors. Beacon messages are leveraged to create a covert channel where the exchanging pseudonyms are inserted into deliberately corrupted beacons. Normal nodes upon receiving corrupted beacons will discard the packets; however, the intended nodes having the shared secrets with the sender, extract the secret information, i.e. pseudonym from the corrupted packet. Our proposed scheme is secure, robust, efficient, and preserves conditional privacy with an efficient revocation mechanism. As a future work, we aim to add a covert module for pseudonym exchange in the current simulators.

Acknowledgment

This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support programs (IITP-2015-H8501-15-1007, IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & communications Technology Promotion). This work was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A2A2A01046986). This work was also supported in part by US NSF HRD-1345219 and HRD-1533653.

References

[1] L. Delgrossi and T. Zhang, "Dedicated short-range communications," *Vehicle Safety Communications: Protocols, Security, and Privacy*, pp. 44–51, 2009.

[2] B. K. Chaurasia and S. Verma, "Maximizing anonymity of a vehicle through pseudonym updation," in *Proceedings of the 4th Annual International Conference on Wireless Internet*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 83.

[3] R. Hussain, S. Kim, and H. Oh, "Towards privacy aware pseudonymless strategy for avoiding profile generation in vanet," in *Information Security Applications*. Springer, 2009, pp. 268–280.

[4] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in vanets: Identity diffusion using timeslots and swapping," in *Vehicular Networking Conference (VNC), 2010 IEEE*. IEEE, 2010, pp. 174–181.

[5] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 1, pp. 86–96, 2012.

[6] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*. IEEE, 2004, pp. 127–131.

[7] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*. IEEE, 2010, pp. 176–183.

[8] R. Hussain, F. Abbas, J. Son, D. Kim, S. Kim, and H. Oh, "Vehicle witnesses as a service: Leveraging vehicles as witnesses on the road in vanet clouds," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 1, Dec 2013, pp. 439–444.

[9] R. Rivest, "Chaffing and winnowing: Confidentiality without encryption," *Cryptobytes(RSA Laboratories)*, vol. 4, no. 1, pp. 12–17, Firstquarter 1998.

[10] A. Narain, N. Feamster, and A. C. Snoeren, "Deniable liaisons," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 525–536.

[11] J. M. de Fuentes, J. Blasco, A. I. Gonz, and L. Manzano, "Applying information hiding in vanets to covertly report misbehaving vehicles," *International Journal of Distributed Sensor Networks*, vol. 2014, p. 15, 2014.

[12] B. Han, L. Ji, S. Lee, B. Bhattacharjee, and R. Miller, "All bits are not equal - a study of ieee 802.11 communication bit errors," in *INFOCOM 2009, IEEE*, April 2009, pp. 1602–1610.

[13] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 246–250.

[14] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust and efficient anonymous authentication protocol in vanets," *Communications and Networks, Journal of*, vol. 11, no. 6, pp. 607–614, Dec 2009.

[15] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 7, pp. 3589–3603, Sept 2010.

[16] R. Hussain, Z. Rezaeifar, D. Kim, A. Tokuta, and H. Oh, "On secure, privacy-aware, and efficient beacon broadcasting among one-hop neighbors in vanets," in *Military Communications Conference (MILCOM), 2014 IEEE*, Oct 2014, pp. 1427–1434.