Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops

Traceable Anonymous Authentication Scheme for Vehicular Ad-hoc Networks

Zeen Kim, Junhyun Yim, Jangseong Kim, Kwangjo Kim
Dept. of Info. and Comm. Eng.
KAIST
Daejeon, Korea
Email: zeenkim,junhyunv,jskim.withkals,kkj@kaist.ac.kr

Taeshik Shon
Division of Info. and Comp. Eng.
Suwon, Korea
tsshon@ajou.ac.kr

***Abstract*—In this paper, we proposed a novel anonymous authentication scheme in VANETs. Our scheme provides message authentication, anonymity, unlinkability, and traceability of an end-user simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. Compared with the existing work, we claim that our scheme has better performance in terms of storage, computation, and communication overhead.**

***Index Terms*—Vehicular ad-hoc network, anonymous authentication, conditional tracking.**

I. Introduction

Along with the fast improvement and wide deployment of wireless communication technologies, Vehicular Ad-hoc Networks (VANETs) [8] which are one of their typical applications, as a special form of Mobile Ad-hoc Networks (MANETs) [3], provide communications among nearby vehicles and roadside units (RSUs) connected the infrastructure. VANET inherently cannot only provide a perfect way to collect dynamic traffic information, but also collect various physical conditions related to traffic distribution with low cost and high accuracy.

In the VANET, a formidable set of abuses and attacks always happens. We have to consider, for example, an attacker who contaminates the large portions of the vehicular network with false information. A single compromised vehicle can transmit false hazard warnings, which can then be taken up by all vehicles in both traffic streams. A tampered vehicle can forge messages to masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. A malicious attacker can deploy a number of receivers and records messages transmitted by the vehicles. Then, the attacker can infer to the private information about its driver and passengers from recorded messages to track the location of the vehicle. It is clear that security and privacy enhancing mechanisms are necessary to thwart such attacks, which are in fact a prerequisite for deployment. Otherwise VANET systems could make anti-social and criminal behavior easier, in a way that would actually jeopardize the benefits of their deployment. This has been recently well understood in academia, the industry, and among authorities. And a large number of agreed efforts have been undertaken to design security architectures for VANET systems.

Extensive research efforts have been made by both industry and academia to solve this problems and make VANETs secure. Some researches [5], [6], [7], [8], [9] described secure network models and threats in VANETs. And there are privacy preservation and conditional tracking issues. But most of existing schemes for secure vehicular networks [12], [13], [14] were simply for authentication with privacy preservation without an effective and efficient conditional tracking mechanism. When a malicious node is detected in VANETs, the conditional tracking mechanism could be utilized to manage revocation list [10] efficiently. So some researches [15], [16], [17] proposed an anonymous authentication protocol which has the conditional tracking mechanism. Their schemes are based on a huge number of anonymous keys and pure group signature technique. They can fall disadvantage in the aspects of requiring a huge storage for anonymous keys and safety message for anonymous authentication. This problem becomes essentially fatal when the size of the revocation list, which keeps all the revoked anonymous keys, is large.

In this paper, we propose a novel anonymous authentication scheme in VANETs. Our scheme provides authentication, anonymity, unlinkability, and traceability of an end-user simultaneously. The unlinkability which enables privacy preservation and the traceability for tracking are contradictory. Our scheme has better performance in terms of storage, computation, and communication overhead compared to previous work.

II. Related Work

Dedicated Short Range Communications (DSRC)/Wireless Access in a Vehicular Environment (WAVE) [1], [2] standards suite is based on multiple cooperating standards for mobile wireless radio communications mainly developed by the IEEE. DSRC/WAVE is part of Vehicle Infrastructure Integration (VII) initiative by Federal Highway Authority and supports vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications for emerging ITS. DSRC/WAVE systems fill a niche in the wireless infrastructure by facilitating low latency, geographically local, high data rate, and high mobility communications.

X. Lin *et al.* proposed a secure and privacy preserving protocol for vehicular communications called GSIS [16], using

978-0-7695-4429-8/11 $26.00 © 2011 IEEE
DOI 10.1109/ISPAW.2011.67

group signature and identity-based signature techniques to resolve the requirement of a large number of public key certificates. They use the group signature for communication between vehicles. And the identity-based signature scheme is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity. The GSIS provides authentication, anonymity, unlinkability and traceability. In their work, vehicles possess only their own group signing key issued by a trusted group manager, and each vehicle signs a message by using group signature scheme to be authenticated as a legitimate sender of the message. However, although the revocation list is short and easily updated, the time for message verification accompanied with revocation check grows linearly with the number of revoked vehicles in the revocation list. Thus each vehicle has to spend more time on message verification when the size of revocation list is large. Once the safety message is time-aware, this solution may not be feasible due to the long verification process.

R. Lu *et al.* proposed an efficient conditional privacy preservation protocol for secure vehicular communications, called ECPP [17], which issues on-the-fly short-time anonymous certificate to vehicles by using a group signature scheme. Since RSUs can check the validity of the requesting vehicle during the short-time anonymous certificate generation phase, such revocation check by vehicle itself of GSIS is not required. Therefore message verification is more efficient that GSIS. The ECPP provides authentication, anonymity, unlinkability and traceability under the strong assumption that most RSUs will not disclose any internal information without the authorization of the trusted authority. However, due to a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection facilities against malicious attacks. Therefore, it is possible for an attacker to access RSUs and disclose the information in the RSUs. When multiple RSUs are compromised, an attacker can trace the movement of a vehicle by using the information stored in the compromised RSUs, because each RSU stores unchanged pseudonyms for OBUs in ECPP. As a result, ECPP does not provide unlinkability when some RSUs are compromised.

III. Our Scheme

In this section, we propose an traceable anonymous authentication scheme. Our scheme consists of initiation, authentication and key agreement, and conditional tracking mechanism. To design our scheme, we use a traceable ring signature with k-times anonymity as a building block and ECC. Table I describes the notation used in our scheme.

A. Initiation

Let E be an elliptic curve over additive group $\mathbb{G}$ of prime order q, and let G be a generator point. Let $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, and $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q$ be distinct hash function modeled as random oracles. Above parameters will be shared by all entities in VANETs.

TABLE I
NOTATIONS FOR OUR SCHEME

Notation	Description
H_1, H_2, H_3	distinct hash function modeled as random oracles
G	generator point on elliptic curve E
V_i	vehicle that has index number i in a group N
R_k	RSU with identifier ID_{R_k}
GID_N	group identifier of a group N
sk_{CA}, pk_{CA}	CA's private and corresponding public key
sk_{R_k}, pk_{R_k}	R_k's private and corresponding public key
sk_{V_i}, pk_{V_i}	V_i's private and corresponding public key
PK_N	a list of public keys in a group N
K_{R_k,V_i}	short-term shared key between R_k and V_i
$Cert_{R_k}$	RSU R_k's certificate issued by the CA
Sig_{R_k}	normal signature signed by R_k using pk_{R_k}
$\widehat{Sig}_{V_i}$	traceable ring signature signed by vehicle V_i
$E_K(m)$	symmetric-key encryption function with shared key K and message m

When a vehicle V_i is registered to CA, a pair of private and corresponding public keys (sk_{V_i}, pk_{V_i}) are equipped in vehicle's HSM. The key generator picks up random element x_i in $\mathbb{Z}_q$ and computes $y_i = x_i G$. The public key is $pk_{V_i} = y_i$, and the corresponding private key is $sk_{V_i} = x_i$. Next V_i's public key is registered in CA on off-line. The CA classifies newly legitimate vehicle V_i into several new groups depend on the vehicle's attributes. For example, V_i will be classified into group N as $N = \{\cdots, i, \cdots\}$, and vehicle V_i keep the group identifier GID_N. The CA then makes an ordered public key list for group N as $PK_N = \{\cdots, pk_{V_i}, \cdots\}$. After generating new group and those group key lists, CA stores related information of newly registered vehicle such as VIN(Vehicle Identification Number), attributes of vehicle V_i, expiration time, *etc*. In addition, RSU R_k also has its pair of private and public cryptographic keys (sk_{R_k}, pk_{R_k}). Each RSU R_k also has a public key certificate signed by the CA to prove pk_{R_k} valid. The certificate $Cert_{R_k}$ is formed as follows.

$$Cert_{R_k}\text{=}\{ID_{R_k},\ pk_{R_k},\ Expiration\ time,\ location,\ Sig_{CA}$$

Where Sig_{CA} denotes a signature (*e.g.*, ECDSA-160) signed on a given message using the private key of the CA.

B. Authentication and Key Agreement

To access VANETs, a vehicle should authenticate himself to a RSU.

1) The RSU R_k picks a random number $n_k \in \mathbb{Z}_q$ and computes $n_k G$ using a generator G. R_k signs on G, $n_k G$ and current timestamp ts_1 using signing algorithm. R_k then broadcasts the following beacon message:
$$(G,\ n_k G,\ ts_1,\ Sig_{R_k},\ Cert_{R_k}).$$
Each RSU will broadcast this beacon message periodically to declare service existence.
2) After receiving this beacon message, a vehicle V_i proceeds as follows.
    a) First V_i check that ts_1 is valid to prevent from the replay attack. Then, V_i verifies Sig_{CA} in $Cert_{R_k}$ using pk_{CA}, and confirm $Cert_{R_k}$ to verify public

key pk_{R_k}, certificate expiration time, and location of R_k. V_i then verifies Sig_{R_k} using pk_{R_k}.

b) V_i picks a random number n_i, computes n_iG and the short-term shared symmetric key with R_k : $K_{R_k,V_i} = n_i(n_kG)$, and encrypt $(s, issue, GID_N)$ using K_{R_k,V_i} where s is the index which is not used and will be exhausted at this time for generating signature and $issue$ can be an arbitrary string in $\{0,1\}^*$. In this system, $issue$ will be concatenation of the service identifier and the service expiration time of V_i. In addition, $issue$ can be changeable depending on the taste of CA.

c) If all the verifications are confirmed, V_i believes that R_k is legitimate and executes the following:

   i) First V_i picks random number $r \in \mathbb{Z}_q$ and computes rG. Then V_i finds current index s and makes message m as concatenation of n_iG, rG, and current timestamp ts_2. V_i also prepares the tag $L = \{s, issue, PK_N\}$.

   ii) V_i computes $Q = H_1(L)$ and $\sigma_i = x_iQ$, using $x_i \in \mathbb{Z}_q$.

   iii) V_i sets $A_0 = H_2(L, m)$ and $A_1 = i^{-1}(\sigma_i - A_0)$

   iv) For all $j \neq i$ in a group N, V_i computes $\sigma_j = A_0 + jA_1 \in \mathbb{G}$. Note that every $(j, \sigma_j(Q)^{-1})$ are defined by $(0, A_0(Q)^{-1})$ and (i, x_i), where $x_i = \sigma_i(Q)^{-1}$.

   v) V_i makes signature (c_N, z_N) on (L, m) depending on a non-interactive zero-knowledge proof of knowledge for the relation derived from language $\mathscr{L} \overset{\triangle}{=} \{(L, Q, \sigma_N) | \exists i' \in N$ such that $y_{i'}(G)^{-1} = \sigma_{i'}(Q)^{-1}\}$
   where $\sigma_N = (\cdots, \sigma_i, \cdots)$, as follows:

      A) V_i picks up random $w_i \in \mathbb{Z}_q$ and sets $a_i = w_iG$, $b_i = w_iQ \in \mathbb{G}$.

      B) V_i picks up at random z_j, $c_j \in \mathbb{Z}_q$, and sets $a_j = z_jG + c_jy_i$, $b_j = z_jQ + c_j\sigma_j \in \mathbb{G}$ for every $j \neq i$ in a group N.

      C) V_i sets $c = H_3(L, A_0, A_1, a_N, b_N)$ where $a_N = (\cdots, a_i, \cdots)$ and $b_N = (\cdots, b_i, \cdots)$.

      D) V_i sets $c_i = c - \sum_{j \neq i} c_j \ (mod\ q)$ and $z_i = w_i - c_ix_i \ (mod\ q)$. V_i then generates (c_N, z_N), where $c_N = (\cdots, c_i, \cdots)$ and $z_N = (\cdots, z_i, \cdots)$, as a proof of $\mathscr{L}$.

d) V_i generates $\widehat{Sig}_{V_i} = (A_1, c_N, z_N)$ as the signature on (L, m).

e) V_i sends the following back to R_k:
$(E_{K_{R_k,V_i}}(s, issue, GID_N), n_iG, rG, ts_2, \widehat{Sig}_{V_i})$.
Where $E_K(m)$ denotes encrypted message by symmetric-key encryption function (*e.g.*, AES-128) whose parameters are shared key K and message m.

3) After receiving this message from vehicle V_i, R_k carries out the following to authenticate V_i.

   a) R_k verifies ts_2 and rG to make sure the freshness of this message from V_i.

   b) R_k computes the short-term shared symmetric key with V_i as $K_{R_k,V_i} = n_k(n_iG)$, and decrypts $E_{K_{R_k,V_i}}(s, issue, GID_N)$.

   c) R_k sends to CA $(ID_{R_K}, s, issue, GID_N, n_iG, rG, ts_2, \widehat{Sig}_{V_i})$, and receives response (GID_N, PK_N) from CA.

   d) R_k parses L as $\{s, issue, PK_N\}$ and also checks s by confirming $1 \leq s \leq k$ where k is the maximum index number of V_i.

   e) R_k verifies that $\widehat{Sig}_{V_i}$ is valid signatures as follows:

      i) R_k checks $G, A_1 \in \mathbb{G}$, $c_i, z_i \in \mathbb{Z}_q$, and $y_i \in \mathbb{G}$ for all $i \in N$. R_k sets $Q = H_1(L)$ and $A_0 = H_2(L, m)$, and compute $\sigma_i = A_0 + iA_1 \in \mathbb{G}$ for all $i \in N$.

      ii) R_k computes $a_i = z_iG + c_iy_i$ and $b_i = z_iQ + c_i\sigma_i$ for all $i \in N$.

      iii) R_k verifies that $H_3(L, m, A_0, A_1, a_N, b_N) \equiv \sum_{i \in N} c_i \ (mod\ q)$, where $a_N = (\cdots, a_i, \cdots)$ and $b_N = (\cdots, b_i, \cdots)$.

      iv) If all the verifications are finished successfully, R_k believes V_i is legitimate vehicle and accepts their access to the network, otherwise rejects.

   f) R_k sends the following back to V_i:

$$(rG, E_{K_{R_k,V_i}}(R_k, rG)).$$

This protocol can authenticate explicitly each other between legitimate vehicle and RSU. In addition, it enables anonymous authentication and establish a short-term shared symmetric key K_{R_k,V_i} that will be used for the subsequence communication session. Each session is uniquely defined as (rG).

C. Conditional Tracking Mechanism

In our scheme, only CA can revoke the anonymity of the vehicle and track the target vehicle. When the CA decides the target vehicle, the CA obtains the public key of the target vehicle and real identity, and link related records as follows:

1) RSUs report the record with $(ID_{R_K}, s, issue, GID_N, n_iG, rG, ts_2, \widehat{Sig}_{V_i})$ to CA in the authentication process.
2) The CA parses L as $\{s, issue, PK_N\}$, and sets message m concatenation of n_iG, rG, and ts_2.
3) The CA sets $Q = H_1(L)$ and $A_0 = H_2(L, m)$, and compute $\sigma_i = A_0 + iA_1 \in \mathbb{G}$ for all $i \in N$. The CA also does the same computation for σ', and retrieve σ'_i for all $i \in N$.
4) For all $i \in N$, if $\sigma_i = \sigma'_i$, store pk_{V_i} in **List**, where **List** is initially an empty list.
5) If public key is the only entry in **List**, the CA can determine an identifier of the target vehicle and obtain its public key.

Since CA has the vehicle's identity, public key pair, and linked authentication records, the CA can revoke the anonymity of the target client, obtain the real identity of vehicle, and track the target vehicle. We utilize a tag-linkability [18] which is property of traceable ring signature to track the target vehicle. The tag-linkability is that every two signature generated by the same signer with the same tag are linked. Our scheme utilize the k-time anonymity using index value s to provide unlinkability with traceability. So we use the vehicle's real identity and the corresponding public key to connect related linked records.

IV. Security Analysis

A. Authentication

Our scheme provides authentication of message and sender of message using signature on message and corresponding public key. Especially, vehicles identify RSUs using certificates issued by the CA. So, no adversary can try impersonation attack, message forgery, and related attacks. In our scheme, even though an attacker compromises some RSUs or vehicles, the attacker cannot forge a message and signature in a communication range of compromised RSUs or vehicles.

B. Anonymity

Our scheme utilizes the traceable ring signature to satisfy the anonymity. As long as a signer does not sign on two different messages with the same tag, the identity of the signer is indistinguishable from any of the possible ring members. In addition, any two signatures generated with two distinct tags are always unlinkable. Namely, it is infeasible for anyone to determine whether they are generated by the same signer. CAs have only negligible advantage to determine which is client among all members in a same group compared with the probability of just guessing randomly one among all members in a same group.

C. Unlinkability

An eavesdropper cannot link the safety messages, because our scheme use k-times anonymity on the same tag. Any traceable ring signature scheme can be efficiently transformed into a traceable ring signature scheme with k-times anonymity, where the k-times anonymity means that a singer is allowed to sign messages with the same tag at most k times without being traced. It is simply obtained by regarding $(i, \textbf{Sig}_{sk}((L, i), m))$ as a signature on m, with the tag L, where the verifier checks if $\textbf{Ver}((L, i), m) = 1$ and $1 \leq i \leq k$. It is obvious that the identity of signer is not revealed if the signer is sufficiently smart not to issue the same index twice on the same tag. Our scheme utilizes an index value s that is changeable in the tag L to provide unlinkability utilizing k-times anonymity. So, signatures generated by same vehicle with the different tag which is changeable are not linked and received messages from same vehicles in authentication process also have unlinkability. Moreover, even though the adversary compromised RSUs, nobody can link information stored in the RSUs to track vehicles.

D. Traceability

Our scheme provides traceability using tag-linkability which is property of traceable ring signature. Anyone who creates two signatures for different message with the same tag can be traced due to tag-linkability. When the CA decides the target vehicle, the CA can revoke the anonymity of the target vehicle and obtain the real identity of vehicle, because CA stores the vehicle's identity and public key pair. CA then traces the target vehicle using tag-linkability property. In addition, even if multiple RSUs are compromised, the authority can trace real identities of target vehicles from its pseudo identity without assistance of compromised RSUs.

V. Performance Analysis

We conducted analysis of our scheme in terms of storage, computation, and communication overhead with comparing previous schemes: M. Raya *et al.*'s model [15], X. Lin *et al.*'s GSIS [16], and R. Lu *et al.*'s ECPP [17]. For the performance analysis, we estimate the required storage units, the required time for computation, and the number of message transmissions.

A. Storage Overhead

We compare the vehicle storage overhead of the our scheme with previous schemes. In our scheme, each vehicle stores one unique private key issued by the CA. Let each key (with its certificate) occupy one storage unit. Then, since the vehicle does not need to store the revocation list, the storage overhead of our scheme is only one unit, denoted as $\mathbf{S}_{Ours} = 1$. In M. Raya *et al.*'s model, on the other hand, each vehicle should store not only its own N_{okey} anonymous key pairs, but also all the anonymous public keys and their certificates in the revocation list. Assuming that there are n vehicles being revoked, then the size of revoked anonymous public keys is $n \times N_{okey}$. The storage overhead of M. Raya *et al.*'s model increases linearly, denoted as $\mathbf{S}_{Raya} = (n+1) \times N_{okey}$. By assuming that $N_{okey} = 10^4$ as mentioned in [15], we have $\mathbf{S}_{Raya} = (n+1) \times 10^4$. In GSIS, each vehicle stores one unique private key issued by the CA, and n revoked public keys in the revocation list. So storage overhead of GSIS is denoted as $\mathbf{S}_{GSIS} = n + 1$. In ECPP, each vehicle stores one unique private key issued by the CA and short-time key pair together with its certificate issued by the RSU. Because vehicle does not need to store the revocation list, the storage overhead in ECPP of denoted as $\mathbf{S}_{ECPP} = 2$.

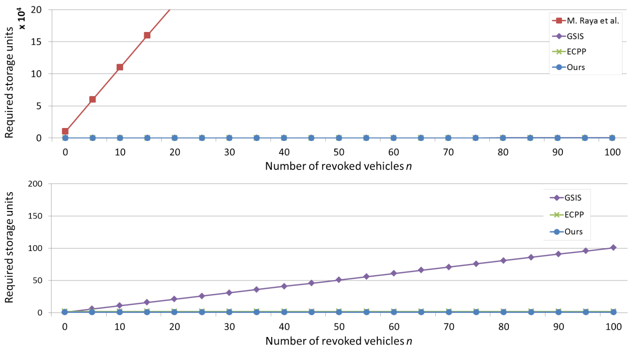

Fig. 1. Comparison of storage overhead in different n revoked vehicles

Figure 3 shows the required storage units in vehicle for our scheme, ECPP, GSIS, and M. Raya *et al.*'s model as n

increases, n varying from 0 to 300. We can observe that the storage overheads of M. Raya *et al.*'s model and GSIS increase linearly with the number of revoked vehicles n. Since the storage overhead of M. Raya *et al.*'s model is much larger than the storage overhead of GSIS, the storage overhead of GSIS looks like still small in spite of its linear increase with n. Therefore, it also implies that the vehicles in M. Raya *et al.*'s model and GSIS would take a long time to update their local revocation lists, which is not the case in our scheme and ECPP. The storage overhead of our scheme and ECPP are always only one and two storage units, and does not increase with the number of revoked vehicles n. Our scheme is said to be the most efficient in terms of vehicle storage overhead, though difference is very small. In addition, ECPP does not provide unlinkability when some RSUs were compromised.

B. Computation Overhead

In this subsection, we compare the computation overhead for mutual authentication in our scheme with previous schemes: GSIS and ECPP. To investigate the performance issue, we calculate the time for computation. Since the point multiplication in $\mathbb{G}$ and pairing computations dominates each party's computation overhead, only these operations are counted in the calculation. For fairness in comparisons, we selected the same security measures of [17]. We assumed an MNT curve [20] of embedding degree $k = 6$ and $|q| = 160\ bit$. The implementation was executed on an Intel Pentium IV 3.0 GHz machine.

TABLE II
CRYPTOGRAPHIC OPERATION'S EXECUTION TIME

	Description	Time
$\mathbf{T}_{pmul}$	The time for one point multiplication in $\mathbb{G}$	0.6 ms
$\mathbf{T}_{pair}$	The time for pairing operation	4.5 ms

Table II gives the measures to estimate the computation time. The computation overhead of our scheme depends on on the group size N, and some variables can be precomputed for the optimization. For the calculation, we set $N = 10$, which can guarantee proper level of anonymity and signature length. In this case, our scheme requires $70\mathbf{T}_{pmul}$ for mutual authentication and verification of message. Let $\mathbf{T}_{Ours}$ be the required time cost in our scheme, then we have: $\mathbf{T}_{Ours} = 70\mathbf{T}_{pmul} = 70{\times}0.6 = 42\ ms$. In ECPP, for mutual authentication, short-time anonymous certificate issuance, and verification of message, it requires $24\mathbf{T}_{pmul} + 9\mathbf{T}_{pair}$. Let $\mathbf{T}_{ECPP}$ be the required time cost in ECPP, then we have: $\mathbf{T}_{ECPP} = 24\mathbf{T}_{pmul} + 9\mathbf{T}_{pair} = 24{\times}0.6 + 9{\times}4.5 = 54.9\ ms$. In GSIS, the time cost of verifying a safety message is related to the number of revoked vehicles in the revocation list. Let $\mathbf{T}_{GSIS}$ be the required time cost in GSIS. Assume that there are n revoked vehicles, then we have: $\mathbf{T}_{GSIS} = 6\mathbf{T}_{pmul} + (3+2n)\mathbf{T}_{pair} = 6{\times}0.6 + (3+2n){\times}4.5 = 3.6 + 13.5 + 9n = (17.1 + 9n)\ ms$.

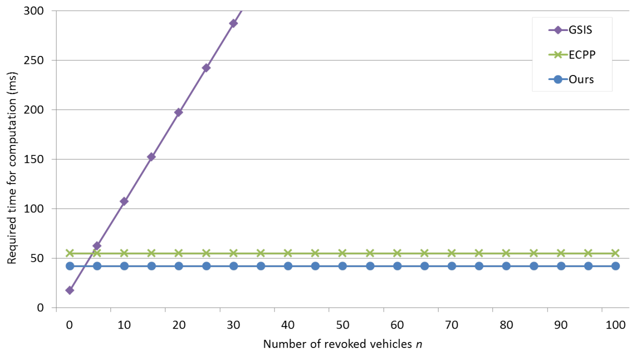

Fig. 2. Comparison of computation overhead in different n revoked vehicles

Figure 4 shows the comparison of computation overhead for authentication and message verification process in our scheme, ECPP, and GSIS as the number of vehicles n increases. We can observe that the computation overhead of GSIS linearly increases with n. On the other hand, computation overheads of our scheme and ECPP are constant. But, our scheme is the most efficient in terms of computation overhead, because ECPP require more time for computation than ours. In addition, ECPP has additional exponentiation operations.

C. Communication Overhead

In this subsection, to analyze communication overhead of our scheme, we estimate the number of message transmissions for mutual authentication and compare the required total number of message transmissions for mutual authentication and message exchanges between the vehicle which was authenticated by the RSU and the RSU which was authenticated by the vehicle in our scheme with other previous schemes: GSIS and ECPP.

TABLE III
COMPARISON OF THE NUMBER OF MESSAGE TRANSMISSIONS FOR MUTUAL AUTHENTICATION

	Ours	GSIS	ECPP
Vehicle	1	1	2
RSU	3	2	3
CA	1	1	1
Total	5	4	6

Table III shows the comparison of the required number of message transmissions for mutual authentication in each scheme. Each scheme has one message exchange between RSU and CA to get vehicle's group public key or confirm updated revocation list. GSIS requires only four message transmissions for mutual authentication, but needs additional message transmissions sometimes to update revocation list. Since GSIS has same authentication process for all messages, GSIS requires $4n$ message transmissions for n times message exchanges between the vehicle which was authenticated by the RSU and the RSU which was authenticated by the vehicle.

Let $\mathbf{C}_{GSIS}$ be the communication overhead of GSIS, the communication overhead of GSIS is denoted as $\mathbf{C}_{GSIS} = 4n$. On the other hand, our scheme and ECPP require $2n$ message transmissions to exchange n messages, because they use result of authentication to exchange messages. ECPP uses short-time certificate issued by the RSU and location awareness key to authenticate messages, and our scheme uses short-term shared key to authenticate and protect messages. However, ECPP and GSIS don't have message eavesdropping protection mechanism such as payload encryption. Let $\mathbf{C}_{Ours}$ and $\mathbf{C}_{ECPP}$ be the communication overhead of our scheme and ECPP, the communication overheads in our scheme and ECPP are denoted as $\mathbf{C}_{Ours} = 5 + 2n$ and $\mathbf{C}_{ECPP} = 6 + 2n$.

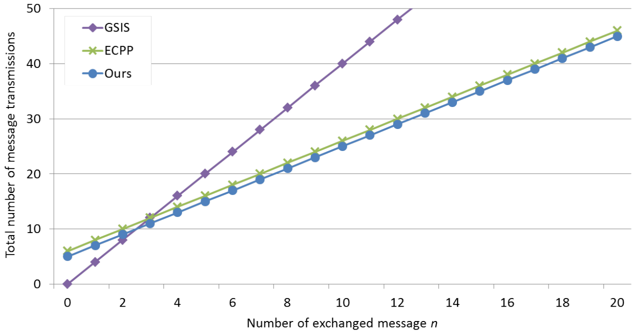

Fig. 3. Comparison of communication overhead in different n message exchanges

Figure 5 shows the total number of message transmissions with growing of the number of exchanged messages n when the vehicle communicate with the same RSU. The total numbers of message transmissions in each protocol are linearly increase with growing of n. Especially, the total number of message transmissions in GSIS increases in multiples of four, but total numbers of message transmissions in our scheme and ECPP increase in multiples of two. The difference between GSIS and the others grows with increasing of the number of message exchanges. Our scheme is the most efficient in terms of communication overhead, although there is slight difference compared with ECPP.

VI. Conclusion

In this paper, we proposed a novel anonymous authentication scheme in VANETs. Our scheme guarantees authentication, anonymity, unlinkability, and traceability simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. Compared with existing works, our scheme has better performance in terms of storage, computation, and communication overhead. In addition, our scheme has three advantages compared with other previous works. First, our scheme doesn't have revocation list update process in authentication process. Second, our scheme always provides unlinkability although multiple RSUs are compromised. Finally, our scheme requires only one authentication process for mutual authentication when the vehicle communicate with the same RSU, because our scheme has key agreement functionality that makes secure channel to communicate.

Acknowledgement

Previous version of this work was presented at WISA 2009. This work is an extended work of WISA 2009 paper.

References

[1] *"Dedicated Short Range Communications (DSRC)"*, Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] L. Morgan, *"Notes on DSRC and WAVE Standards Suite, Its Architecture, Design, and Characteristics"*, IEEE Communications Surveys & Tutorials, 2010.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, *"Security in Mobile Ad Hoc Networks: Challenges and Solutions"*, IEEE Wireless Communications, Vol. 11, Issue 1, pp. 38-47, 2004.

[4] F.Y. Wang, D. Zeng, and L. Yang, *"Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update"*, IEEE Pervasive Computing, Vol. 5, Issue 4, pp. 68-69, 2006.

[5] M. Raya, *"The Security of Vehicular Ad Hoc Networks"*, in Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 11-21, Alexandria, VA, USA, November 2005.

[6] M. Raya, P. Papadimitratos, and J.P. Hubaux, *"Securing Vehicular Communications"*, IEEE Wireless Communications, Vol. 13, Issue 5, pp. 8-15, 2006.

[7] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, *"Securing Vehicular Communications - Assumptions, Requirements, and Principles"*, in Proc. of ESCAR 2006, pp. 5-14, Berlin, Germany, November 2006.

[8] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho, and X.S. Shen, *"Security in Vehicular Ad Hoc Networks"*, IEEE Communications Magazine, Vol. 46, Issue 4, pp. 88-95, 2008.

[9] P. Papadimitratos, A. Kung, F. Kargl, Z. Ma, M. Raya, J. Freudiger, E. Schoch, T. Holczer, L. Buttyan, and J.P. Hubaux, *"Secure Vehicular Communication Systems: Design and Architecture"*, IEEE Communications Magazine, Vol. 46, Issue 11, pp. 100-109, 2008.

[10] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, *"Certificate Revocation List Distribution in Vehicular Communication Systems (short paper)"*, in Proc. of the 5th ACM International Workshop on VANET, San Francisco, CA, USA, September 2008.

[11] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux,*"Secure Vehicular Communications: Implementation, Performance, and Research Challenges"*, IEEE Communcations Magazine, Vol. 46, Issue 11, pp. 110-118, 2008.

[12] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, *"Adaptive Privacy-Preserving Authentication in Vehicular Networks"*, in Proc. of IEEE International Workshop on Vehicle Communication and Applications, October 2006.

[13] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, *"Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks"*, in Proc. of the 8th International Symposium on Autonomous Decentralized Systems (ISADS 2007), pp. 344-351, Sedona, AZ, USA, March 2007.

[14] C. Zhang, R. Lu, P.H. Ho, and A. Chen, *"A Location Privacy Preserving Authentication Scheme in Vehicular Networks"*, in Proc. of WCNC 2008, pp. 2543-2548, 2008.

[15] M. Raya and J.P. Hubaux , *"Securing Vehicular Ad Hoc Networks"*, Journal of Computer Security, Vol. 15, Issue 1, pp. 39-68, 2007.

[16] X. Lin, X. Sun, P.H. Ho, and X. Shen, *"GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications"*, IEEE Transactions on Vehicular Technology, Vol. 56, Issue 6, pp. 3442-3456, 2007.

[17] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, *"ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications"*, in Proc. of INFOCOM 2008, pp. 1229-1237, April 2008.

[18] E. Fujisaki and K. Suzuki, *"Traceable Ring Signature"*, PKC 2007, LNCS 4450, pp. 181-200, 2007.

[19] I. Teranishi, J. Furukawa, and K. Sako, *"k-Times Anonymous Authentication"*, Advances in Cryptology - ASIACRYPT 2004, LNCS 3329, pp. 308-322, 2004.

[20] A. Miyaji, M. Nakabayashi, and S. Takano, *"New Explicit Conditions of Elliptic Curve Traces for FR-Reduction"*, IEICE Transactions on Fundamentals, Vol. E84-A, Issue 5, pp. 1234-123, 2001.