An Efficient Anonymous Authentication Protocol in Vehicular Ad-hoc Networks

Junhyun Yim, Imsung Choi, and Kwangjo Kim

Korea Advanced Institute of Science and Technology
{junhyunv,choiimsung,kkj}@kaist.ac.kr

Abstract. In this paper, we introduce an efficient anonymous authentication protocol in Vehicular Ad-hoc Networks (VANETs) [5] to resolve the issue on anonymous authentication for communication between roadside units and vehicles. Our proposed protocol cannot only guarantee privacy, anonymity, and other basic cryptographic requirements but also provide traceability of illegal users. Our proposed protocol utilizes the traceable ring signature scheme [12] and the k-times anonymous authentication scheme [13] to address the contradiction between the anonymity and traceability.

1 Introduction

Along with the improvement and wide spread of wireless communication technologies, Vehicular Ad-hoc Networks (VANETs) which are one of their typical applications, as a special form of Mobile Ad-hoc Networks (MANETs) [24], provide communications among nearby vehicles and between vehicles and roadside units (RSUs) connected infrastructure. VANET inherently can provide a perfect way to collect dynamic traffic information and sense various physical conditions related to traffic distribution with very low cost and high accuracy, which is considered to be essential for achieving automatic and dynamic information collection and fusion in an Intelligent Transportation System (ITS) [2]. VANETs have a great potential to revolutionize driving environment, and will undoubtedly play an important role in the future transportation system. Recently, the growing demand for optimization of road traffic and improvement of road safety has brought a wide interest on VANETs. Therefore car manufactures and telecommunication industries prepare to equip each vehicle with wireless devices that allow vehicle-to-vehicle and vehicle-to-RSU communication in order to improve driver's driving experience and safety.

A VANET system mainly consists of vehicles, roadside units (RSUs) and Certificate Authorities (CAs). Vehicles have wireless communication and computation devices, While RSUs connected with infrastructure are deployed in roadside to provide wireless communication to vehicles within their radio converges. According to the Dedicated Short Range Communications (DSRC)[1] protocol, each vehicle in a VANETs broadcasts a traffic safety message every 100-300ms, which keeps the vehicle's driving related information, such as location, speed, turning intention, and driving status (*e.g.*, regular driving, waiting

for a traffic sign, traffic jam, *etc.*) to other vehicles. With multi-hop forwarding, the messages will be either terminated by a vehicle or dropped when exceeding over their lifetimes. When receiving a message, the vehicle can either react to it if the sending vehicle of the message is nearby with some requests that can be handled locally, or deliver the information to a traffic control center if the message is considered to contain any useful information. The vehicle can also monitor the traffic situation of its current location and report the summarized information to the traffic control center. The traffic control center can generate an optimized control and management strategy for traffic sign control by analyzing the current traffic load in each intersection, in addition to traffic information collection for traffic flow analysis and control.

In the system, a formidable set of abuses and attacks always happen. We have to consider, for example, an attacker that 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 different type of attacker can deploy a number of receivers and records messages transmitted by the vehicles. Especially safety beacons that report the vehicle's location. So an attacker can infer to the private information about its driver and passengers to track the location of vehicle. It is clear that to thwart such attacks, security and privacy enhancing mechanisms are necessary, 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 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. But most of the existing schemes [14], [15] for secure vehicular networks were simply for authentication with privacy preservation without an effective and efficient conditional tracking mechanism. Their schemes are based on a huge number of anonymous keys and pure group signature technique. They 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 [7], which keeps all the revoked anonymous keys, is large. Note that when a signature is being verified, the validity of the public key should also be authenticated, however which is not as easy in the vehicular networks as that in wired networks. But traceability can be a good solution which can manage the revocation list efficiently.

In this paper, we propose a novel anonymous authentication in VANETs. It cannot only guarantee privacy, anonymity, and other basic cryptographic requirements but also provide traceability. Our protocol utilizes the traceable ring signature scheme and the k-times anonymous authentication scheme to address the contradictory requirements between the anonymity and the traceability.

The remainder of the paper is organized as follows: A brief survey on the related work is conducted in Section 2. The preliminaries of the proposed authentication protocol are presented in Section 3. In Section 4, the proposed authentication protocol is described in detail. Section 5 analyzes the security and performance of the proposed protocol. The paper is concluded in Section 6.

2 Related Work

In this section, we briefly introduce the existing anonymous authentication scheme for the VANETs.

X. Lin *et al.* proposed a secure and privacy preserving protocol for vehicular communications [10] based on group signature [18] and identity based signature techniques [19], called GSIS. Their scheme guarantees privacy, anonymity, and other basic cryptographic requirements. And also provide traceability of each vehicle. The identity of the message sender is revealed by the authority when any dispute happens. They use the group signature for communication between vehicle and other vehicle. And the identity based signature scheme is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity. But this protocol has vulnerabilities deal with vehicle movement tracking [10] when many of the RSUs are captured by attacker.

R. Lu *et al.* proposed an efficient conditional privacy preservation protocol for secure vehicular communications based on bilinear pairing, called ECPP [9]. Their protocol guarantees privacy, anonymity, and other basic cryptographic requirements. And also provide traceability. But this protocol has vulnerabilities deal with vehicle movement tracking when many of the RSUs are captured by attacker. It is characterized by the generation of on-the-fly short-time anonymous keys between vehicle and RSU. And it can efficiently deal with the growing revocation list by providing traceability. But it has a large overhead for generating the anonymous key and communication.

C. Zhang *et al.* proposed a location privacy preserving authentication scheme [8] based on blind signature in the elliptic curve domain. The scheme can provide fast re-authentication, and guarantee privacy, anonymity, and other basic cryptographic requirements. But it doesn't provide traceability. In order to preserve the user location privacy, they use the BLS short signature [17], which is employed to hide the identity and the trajectory of a vehicle. The location privacy preserving authentication scheme consider re-authentication when vehicle has handover process in between RSU and the other RSUs. So it has fast re-authentication method. However, they must have communication between vehicle and CA when the initial authentication with RSU. This process has a very large communication overhead.

Different from these schemes, we propose a novel efficient anonymous authentication scheme. Our scheme guarantees privacy, anonymity, and other basic cryptographic requirements. And also provide traceability. Authentication schemes in VANETs require anonymity and privacy preserving. At the same time, it needs to provide traceability to retrieve a vehicle's real identity from

its pseudo identity when the signature is in dispute or when the content of a message is bogus. Additionally, our scheme has a better performance than other existing schemes.

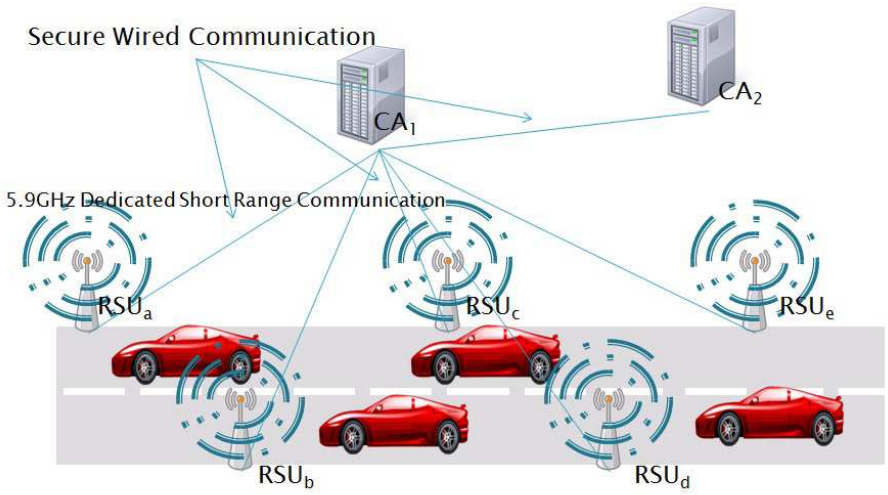

Fig. 1. Abstract View of the VANETs

3 Preliminaries

3.1 System Model

VANETs has three entities such as CA, RSU, and vehicle. In this model, CA is in charge of the registration of immobile RSUs at the road side and vehicles. And RSUs are subordinated by the CA, which have storage units for storing information coming from the CA and the vehicles. It works like CA's gateway.

Because the secure vehicular communications are mainly served for the public applications, in the most highway scenarios, RSUs are assumed to connect with the CA by wired links or any other links with high bandwidth, low delay and low bit error rates [20]. RSU also communicate to each other either via the CA or through a secure and reliable peer-to-peer channel. According to [1], the medium used for communications between neighboring vehicles and between vehicle and RSU is 5.9GHz Dedicated Short Range Communication (DSRC) identified as IEEE 802.11p.

In this system, some assumptions must be made. First, CAs are fully trusted by all parties in the system. And they are infeasible for any attacker. Second, RSUs are immobile and subordinated by the CAs in the most scenarios. Without

the authorization of the CAs, most RSUs will not disclose any inner information. However, we do not exclude a fraction of RSUs at roadside that may be compromised by an attacker and in collusion with each other. Third, vehicles move most of time, and could be easily compromised by a malicious attacker. Compared with the RSUs, the population of the vehicles in the system could be up to millions, whereas the number of RSUs is at most tens of thousands based on the national infrastructure construction.

3.2 Certificate Authority

Drawing from the analogy with existing administrative processes and automotive authorities (*e.g.*, city or state transit authorities), we assume that a large number of Certification Authorities (CAs) will be instantiated. Each CA is responsible for a region (national territory, district, county, *etc.*) and manages identities and credentials of all nodes registered with it. To enable interactions between nodes from different regions, CAs provide certificates for other CAs (cross-certification) or provide foreigner certificates to vehicles that are registered with another CA when they cross the geographical boundaries of their region [21].

3.3 Node Identification

Each vehicle is registered with only one CA, and has a unique long-term identity and a pair of private and public cryptographic keys, and long-term identity and key pair are equipped with a long-term certificate. A list of vehicle attributes and a lifetime are included in the certificate that the CA issues upon vehicle registration and upon certificate expiration. The CA is also responsible for the eviction of vehicles or the withdrawal of compromised cryptographic keys via the revocation of the corresponding certificates. In all cases, the interaction of vehicles with the CA is rare and intermittent, with the roadside infrastructure acting as a gateway to and from the vehicular part of the network, with the use of other infrastructure (*e.g.*, cellular) being also possible. The in-car system and data processing functionality are discussed in [22].

3.4 HSM(Hardware Security Module)

We envision that both vehicles and RSUs are equipped with HSM [3], whose purpose is to store and physically protect sensitive information and provide a secure time base. This information is primarily private keys for signature generation. If modules were tampered with to extract private keys, the physical protection of the unit would ensure that the sensitive information (private keys) would be erased to prevent the adversary from obtaining them. In addition, the HSM performs all private key cryptographic operations with the stored keys, in order to ensure that sensitive information never leaves the physically secured HSM environment. Essentially, the HSM is the basis of trust. Without HSM, private keys could be compromised and their holders could masquerade as legitimate system nodes.

3.5 Security Requirements

Our proposed anonymous authentication protocol should satisfy the following requirements.

1. **Identity anonymity:** The identity of vehicles should be transparent to RSUs when an authentication procedure is processed. This can prevent RSUs from mapping a vehicle's identity with its location.

2. **Movement tracking avoidance:** The moving route of a particular vehicle should be protected, even if the identities are hidden. For example, RSUs should not be able to figure out the relationship between the vehicle and the RSU from which the vehicle is handed over when the authentication is processed. The final objective is that the probability of tracing the vehicle by all compromised RSUs after multiple handover [8] processes should be very small.

3. **Traceability:**The CA should have the ability to retrieve a vehicle's real identity from its pseudo identity when the signature is in dispute or when the content of a message is bogus. The traceability can be solution for large revocation list.

4 Our Proposed Scheme

In this section, we propose an efficient anonymous authentication protocol. To design our proposed scheme, we use a traceable ring signature with k-times anonymity as a building block.

4.1 Initiation

Let $\mathbb{G}$ be a multiplicative group of prime order q and leg g be a generator of $\mathbb{G}$. 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.

When a vehicle v is registered to CA, a pair of private and public cryptographic keys (sk_v, pk_v) are equipped in vehicle's HSM. HSM picks up random element x_i in $\mathbb{Z}_q$ and computes $y_i = g^{x_i}$. The public key of $pk_v = \{g, y_i, G\}$ and the corresponding secret key is $sk_v = \{pk_v, x_i\}$. Next v's public key is registered in CA on off-line.

The CA classifies newly legitimate vehicle v into several new groups depend on the vehicle's attributes. For example, v will be classified into group X as $X = \{\cdots, v, \cdots\}$. The CA then makes an ordered public key list for group X as $pk_X = (\cdots, pk_v, \cdots)$. After generating new group and those group key lists, and related information such as VIN(Vehicle Identification Number), store attribute of vehicle v, expiration time and etc to newly registered vehicle.

In addition, RSU R_k also has its a 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} vaild. The certificate $Cert_{R_k}$ is formed as follows.

$$Cert_{R_k}=\{R_k,\ pk_{R_k},\ Expirationtime,\ Sig_{sk_{CA}}\}$$

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

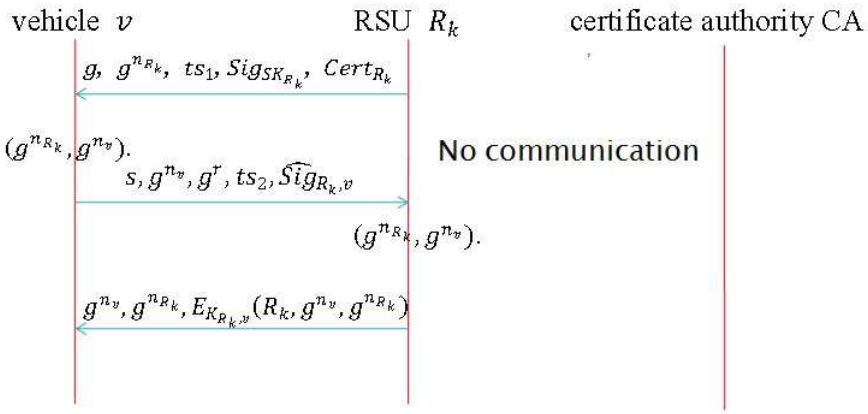

Fig. 2. Abstract View of Authentication and Key agreement

4.2 Authentication and Key agreement

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

1. The RSU R_k picks a random number $n_{R_k} \in \mathbb{Z}_q^*$ and a random generator g in $\mathbb{G}$ and computes $g^{n_{R_k}}$. R_k signs on g, $g^{n_{R_k}}$ and current timestamp ts_1 with signing algorithm. R_k then broadcasts following beacon message.

   $$g,\ g^{n_{R_k}},\ ts_1,\ Sig_{sk_{R_k}},\ Cert_{R_k}$$

   Each RSU will broadcast this beacon message periodically to declare service existence.
2. After receiving this beacon message, a vehicle v proceeds as follows.
   (a) First v verifies that ts_1 is valid to prevent replay attack. Then v confirms $Cert_{R_k}$ to verify pk_{R_k} and the certificate expiration time. Also v verifies $Sig_{sk_{R_k}}$ using pk_{R_k} and matching it.
   (b) If all the verifications are positive, v believes that R_k is legitimate and executes the following:

i. First v picks two random number n_v, $r \in \mathbb{Z}_q^*$ and computes g^{n_v}, g^r. Then v finds current index s and makes m as concatenation of s, g^{n_v}, g^r and current timestamp ts_2. v also prepares the tag $L = \{s, issue, pk_X\}$, 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 $\{0,1\}^*$ and in case of v, $issue$ will be concatenation of the group identifier X and the service expiration time of v. $issue$ can be changeable depending on the taste of CA.

ii. v computes $h = H_1(L)$ and $\sigma_v = h^{x_v}$, using $x \in \mathbb{Z}_q$.

iii. v sets $A_0 = H_2(L, m)$ and $A_1 = (\sigma_v / A_0)^{1/v}$

iv. For all $i \neq v$ in group X, v computes $\sigma_i = A_0 {A_1}^i \in X$. Note that every $(i, log_h(\sigma_v))$ are defined by $(0, log_h(A_0))$ and (v, x_v), where $x_v = log_h(\sigma_v)$.

v. v makes signature (c_X, z_X) on (L, m), depend on a non-interactive zero-knowledge proof of knowledge for the relation derived from language $\mathscr{L} \triangleq \{(L, h, \sigma_X) | \exists v' \in X$ such that $log_g(y_{v'}) = log_h(\sigma_{v'})\}$ where $\sigma_X = (\cdots, \sigma_v, \cdots)$, as follows: v first picks up random $w_v \in \mathbb{Z}_q$ and sets $a_v = q^{w_v}$, $b_v = h^{w_v} \in \mathbb{G}$. Second, v picks up at random z_i, $c_i \in \mathbb{Z}_q$, and sets $a_i = q^{z_i} {y_v}^{c_i}$, $b_i = h^{z_i} {\sigma_i}^{c_i} \in \mathbb{G}$ for every $i \neq v$. Next, v sets $c = H_2(L, A_0, A_1, a_X, b_X)$ where $a_X = (\cdots, a_v, \cdots)$ and $b_X = (\cdots, b_v, \cdots)$. Finally, v sets $c_v = c - \sum_{i \neq v} c_i \ (mod\ q)$ and $z_v = w_v - c_v x_v \ (mod\ q)$. v then generates (c_X, z_X), where $c_X = (\cdots, c_v, \cdots)$ and $z_X = (\cdots, z_v, \cdots)$, as a proof of $\mathscr{L}$.

(c) v generates $\widehat{Sig}_{R_k,v} = (A_1, c_X, z_X)$ as the signature on (L, m).

(d) v computes the shared symmetric key with R_k : $K_{R_k,v} = (g^{n_{R_k}})^{n_v}$.

(e) v sends back to R_k.

$$s, g^{n_v}, g^r, ts_2, \widehat{Sig}_{R_k,v}$$

3. After receiving this message from v. R_k carries out the following to authenticate v.

(a) R_k verifies ts_2 and g^r to make sure the freshness of this message from v and also check s by confirming $1 \leq s \leq k$ where k is the access number of v at maximum.

(b) R_k verifies that $\widehat{Sig}_{R_k,v}$ is valid signatures as follows:

i. R_k generates L as $\{s, issue, pk_X\}$ and checks $g, A_1 \in \mathbb{G}$, $c_i, z_i \in \mathbb{Z}_q$, and $y_i \in \mathbb{G}$ for all $i \in X$.

ii. R_k computes $a_i = g^{z_i} y_i^{c_i}$ and $b_i = h^{(z_i)} {\sigma_i}^{c_i}$ for all $i \in X$.

iii. R_k verifies that $H_2(L, m, A_0, A_1, a_X, b_X) \equiv \sum_{i \in X} c_i \ (mod\ q)$, where $a_X = (\cdots, a_i, \cdots)$ and $b_X = (\cdots, b_i, \cdots)$.

iv. If all the verifications are positive, R_k believes v is legitimate vehicle and accepts their access to the network, otherwise rejects.

(c) R_k further computes the shared symmetric key with v as $K_{R_k,v} = (g^{n_v})^{n_{R_k}}$.

(d) R_k sends back to v

$$g^{n_v}, g^{n_{R_k}}, E_{K_{R_k,v}}(R_k, g^{n_v}, g^{n_{R_k}})$$

Where $E_k(m)$ denotes the output of symmetric encryption of m using the shared key k.

The above protocol can authenticate explicitly each other between legitimate vehicle and RSU. In addition, it enables anonymous authentication and establish a shared symmetric key that will be used for the subsequence communication session. Each session is uniquely defined as $(g^{n_{R_k}}, g^{n_v})$.

5 Analysis

Our proposed scheme, an efficient anonymous authentication protocol in VANETs, satisfies the following requirements.

1. **Identity anonymity:** Our protocol utilizes the traceable ring signature to satisfy the anonymity of vehicle's identity. Theorem 3 of [12] shows the proof of anonymity of vehicle's identity. The used ring signature scheme is anonymous under the decisional Diffie-Hellman assumption in the random oracle model [23]. RSUs and CAs have only negligible advantage to determine which is client among all members in same group compared with the probability of just guessing randomly one among all members in same group.

2. **Movement tracking avoidance:** Our protocol can guarantee anonymity of vehicle's identity and protect vehicle from movement tracking attack. For example, when the vehicle has handover process, the vehicle has re-authentication process too. Then vehicle uses other session key to communicate the other RSU. If many continuous RSU are captured by attacker. Attacker can read some message from vehicles using captured RSUs. In this case, our protocol uses other session key to communication with each RSU. And RSUs can't get information related vehicle's identity because using a different session key for each session. So our protocol satisfies movement tracking avoidance.

3. **Traceability:** When the CA detects the misbehavior of a vehicle, The CA should be able to revoke of the anonymity of the vehicle. When the CA discovers the fraud of a vehicle, the CA obtains the public key of the misbehaved vehicle. Since CA stores the vehicle's identity/public key pair, the CA can revoke the anonymity of the misbehaved client and obtain the client identity.

Our proposed scheme specifies privacy, anonymity, traceability, Movement tracking avoidance, but the other schemes are not. And our proposed scheme has a good efficiency in a view of communication cost. Comparing with other three schemes for VANETs, the proposed protocol has better properties or saving of communication cost.

	X. Lin *et al.*	R. Lu *et al.*	C. Zhang *et al.*	Proposed Scheme
Privacy	O	O	O	O
Anonymity	O	O	O	O
Traceability	O	O	X	O
Location tracking avoidance	X	X	O	O
Communication Cost (Initial)	2	4	7	3
Communication Cost (handover)	2	4	3	3

Fig. 3. Comparing four schemes

6 Conclusion and Future Work

In this paper, we propose an efficient anonymous authentication protocol in VANETs. Our proposed scheme simultaneously specifies all the requirements for anonymous authentication in VANETs. Our protocol uses the traceable ring signature with k-times anonymity as building block. Compared with existing works, our protocol has better properties or saving of communication cost. In addition, our protocol provides k-times anonymity for same tag that does not require any additional communication with the CAs. It is efficient in large-scale and busy networks like VANETs. As future work, we will measure the computational overhead and check the provable security of the proposed protocol. Also an optimal protocol than the proposed one is another research area.

References

1. *"Dedicated Short Range Communications (DSRC)."*, Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.
2. 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, pp. 68-69, 2006.
3. M. Raya, P. Papadimitratos, and J.P. Hubaux, *"Securing vehicular communications"*, IEEE Wireless Communications, vol. 13, pp. 8-15, 2006.
4. M. Raya, *"The security of vehicular ad hoc networks"*, in Proc. the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 11-21, 2005.
5. 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, pp.88-95, 2008.
6. M. Raya and J.P. Hubaux , *"Securing vehicular ad hoc networks"*, Journal of Computer Security, vol. 15, pp. 39-68, 2007.

7. 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, no. 11, 2008, pp. 100-109.
8. C. Zhang, R. Lu, P.H. Ho, and A. Chen, *"NET 18-4-A Location Privacy Preserving Authentication Scheme in Vehicular Networks"*, WCNC, pp. 2543-2548, 2008.
9. R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, *"ECPP: efficient conditional privacy preservation protocol for secure vehicular communications"*, IEEE INFOCOM, pp. 1229-1237, 2008.
10. 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, pp.3442-3456, 2007.
11. P. Papadimitratos, V. Gligor, and J.-P. Hubaux, *"Securing Vehicular Communications - Assumptions, Requirements, and Principles"*, In ESCAR 2006.
12. E. Fujisaki and K. Suzuki, *"Traceable Ring Signature"*, PKC 2007, Lecture notes in computer science vol. 4450, Springer-Verlag, 2007, pp. 181-200.
13. I. Teranishi, J. Furukawa, and K. Sako, *"K-times anonymous authentication"*, in Proc. ASIACRYPT 2004, LNCS 3329, pp. 308-322, 2004.
14. K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, *"Adaptive privacy-preserving authentication in vehicular networks"*, First International Conference on Communications and Networking in China, pp. 1-8, 2006.
15. Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, *"Enforcing privacy using symmetric random key-set in vehicular networks"*, in Prof. of the 8th International Symposium on Autonomous Decentralized Systems (ISADS 2007), pp. 344-351, Sedona AZ, March 2007.
16. A. Aijaz, B. Bochow, D. Florian, A. Festag, M. Gerlach, R. Kroh, and L. Tim, *"Attacks on inter vehicle communication systems - an analysis,"*, In 3nd International Workshop on Intelligent Transportation, Hamburg, Germany, March 2006.
17. D. Boneh, B. Lynn, and H. Shacham, *"Short signatures from the Weil pairing"*, in Proc. Asiacrypt 2001, vol. 2248 of LNCS, Springer-Verlag, pp. 514-532, 2001.
18. D. Chaum and E. van Heijst, *"Group signatures"*, in Proc. Advances in Cryptology - Eurocrypt'91, ser. LNCS, vol. 576, Springer-Verlag, pp. 257-265, 1991.
19. A. Shamir, *"Identity-based cryptosystems and signature schemes,"*, in Proc. Advances in Cryptology - Crypto'84, ser. LNCS, vol. 196. Springer-Verlag, pp. 47-53, 1984.
20. Y. Peng, Z. Abichar, and J.M. Chang, *"Roadside-aided routing (RAR) in vehicular networks"*, in Proc. IEEE ICC 2006, vol. 8, pp. 3602-3607, Istanbul, Turkey, June 2006.
21. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, *"Certificate Revocation List Distribution in Vehicular Communication Systems (short paper)."'*, In ACM VANET, San Francisco, CA, USA, September 2008.
22. 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, November 2008.
23. M. Bellare and P. Rogaway, *"Random oracles are practical: a paradigm for designing efficient protocols"*, ACM CCS 1993, pp. 62-73, Nov. 1993.
24. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, *"Security in mobile ad hoc networks: challenges and solutions"*, IEEE Wireless Communications, 2004.