Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs

Yong Hao, Yu Cheng, and Kui Ren
Dept. of Elec. & Comp. Eng., Illinois Institute of Technology,
Chicago, IL, USA 60616, email: {yhao4, cheng, kren2}@iit.edu

***Abstract*—The group signature based security scheme is a promising approach to provision privacy in vehicular ad hoc networks (VANETs). In this paper, we propose a novel distributed key management scheme for group signature based VANETs, which is expected to considerably facilitate the revocation of malicious vehicles, location privacy protection, heterogenous security policies, and maintenance of the system, compared with the centralized key management assumed by the existing group signature schemes. The distributed nature of the proposed scheme is that the road side units (RSUs) will be responsible for distributing group private keys in a localized manner. A brand-new issue induced by the distributed scheme is that the semi-trust RSUs may be compromised. So we develop security protocols for the distributed key management, which are capable of identifying the compromised RSUs and their collusion with the malicious vehicles if any. Details of possible attacks and the corresponding solutions are discussed to demonstrate the performance of the proposed security protocols.**

I. Introduction

The vehicular ad hoc network (VANET) has been a hot topic in both academia and industry, which provisions interesting and promising functionalities including vehicular safety, traffic congestion avoidance, and location based services [1], [2]. A VANET typically involves two modes of communications, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I).

Privacy is a very important issue in the VANET [3]. As the wireless communication channel is a shared medium, just exchanging messages without any security protection over the air can easily leak the information that the users may want to keep private. There have been several proposals for privacy preservation of VANET. Using pseudonyms is a natural idea to protect the real identity [4]. It is preferable to preserve the location privacy of a vehicle by breaking the linkability between two locations, for which the vehicle can update its pseudonym after each transmission. Considering that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations, the techniques of mix zone [5], silent period [6], and CARAVAN [7] have been proposed to enhance the pseudonym scheme. However, these schemes require the vehicles to store a large number of pseudonyms and certifications, where it is not convenient to implement a revocation scheme to abrogate the malicious vehicle. Moreover, the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and nonrepudiation.

The group signature [8] is a promising security scheme to provision privacy protection in the VANET. A general vehicular communication framework based on group signature is given in [9]. Lin *et. al.* systematically discuss how to implement group signature protocol in the VANET [10]. The work in [11] combines pseudonym schemes with the group signature to avoid storing pseudonyms and certifications in vehicles. To the best of our knowledge, all of the existing group signature schemes are based on centralized key management which has some disadvantages. For example, the system maintenance is not flexible and the revocation is both resource and time consuming.

In this paper, we propose a distributed key management scheme. In our scheme, all the vehicles within the coverage area of a road side unit (RSU) form a group. The RSU acts as the key distributor in the group. When a vehicle approaches an RSU, it will get a group private key from the RSU dynamically. Once, the vehicle gets a group private key, it can send out messages on behalf of the group. Compared to the centralized key management scheme, our scheme has advantages on revocation, location privacy protection, heterogenous security policies implementation and system maintenance. The distributed key management induces a new issue that compromised RSUs may misbehave in the key distribution procedure. These compromised RSUs may collude with malicious vehicles. Therefore, we develop security protocols for the distributed key management, which are capable of identifying the compromised RSUs and their collusion with the malicious vehicles if any. Details of possible attacks and the corresponding solutions are discussed to demonstrate the performance of the proposed security protocols.

The remainder of this paper is organized as follows. Section II introduces system model. Section III describes security protocols which are used to defend compromised RSUs and malicious vehicles from attacking others. Section IV presents possible attacks and performance analysis. Section V gives the conclusion remarks.

II. System Model

A. Group Signature based VANET

Entities in VANET are classified into 3 categories. An illustration of the system and functions of each entity are shown in Fig 1.

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

Network nodes are ordinary vehicles on the road that have ability to communicate with each other through radio. Network nodes have the lowest security level.

Road side infrastructure is the set of RSUs. RSUs are agents of the authority which are deployed at the road sides, for example, traffic lights or road signs can be used as RSUs after renovation. An RSU can be a powerful device or a comparatively simple one. RSI is semi-trust with the medium security level [7].

Authorities are responsible for management in VANET. They hold all the secrets and have responsibilities to solve disputes. The authority has the highest security level. We assume it can not be compromised.

In the group signature scheme, members of a group sign messages under the name of the group. In a group, there are one group public key and many group private keys corresponding to the group public key. A message that is signed by any group private key can be verified by the unique group public key, and the signer's identifier will not be revealed. However, there is an authority who holds a tracing key which can be used to retrieve the group private key from the signature. If one group private key is assigned to only one user, we can identify the user after we get its group private key.

B. Distributed Key Management

In our scheme, the authority generates and holds tracing keys which can be used to recover the identity from the signature. It also chooses group private key generators and transmits them to corresponding RSUs which are in charge of the group private key distribution, such as RSU1 and RSU2 in Fig. 1. A vehicle starts a registration when it is approaching a RSU. The RSU sends a group private key to the vehicle after it gets vehicle's identity information and then stores vehicles' information locally. The authority uses tracing keys to retrieve the identity from the signature if there is a dispute. Thereafter, the authority can get the detailed key distribution records of the accuser and the accused by consulting corresponding RSUs.

Compared with the centralized scheme which preloads keys into the vehicle off-line, our distributed scheme has following advantages. (1) The revocation is more efficient. In our scheme, the revocation list is stored in RSUs. However, in the centralized scheme, revocation list has to be transmitted to every vehicles through wireless channels. Due to the large number of vehicles, the revocation list must be changed quickly. Meanwhile, both adding or deleting an item in the revocation list that distributes in so many vehicles is resource and time consuming. (2) The system maintenance is easier and more flexible. Public key updating is possible in our scheme because group private keys are assigned dynamically. In the centralized scheme, it is nearly impossible to update group public keys. If a group private key is leaked to others, the group private key will be in the revocation list forever. (3) Location privacy protection is improved. In our scheme, vehicles will change their group private keys while traveling on the road. However, in the centralized scheme, vehicles always use the same group private key. The adversary has a higher probability to find that two messages are transmitted by the same sender. (4) Heterogenous security policies can be implemented in our scheme. While, in the centralized scheme, the policy is difficult to be changed after it is deployed.

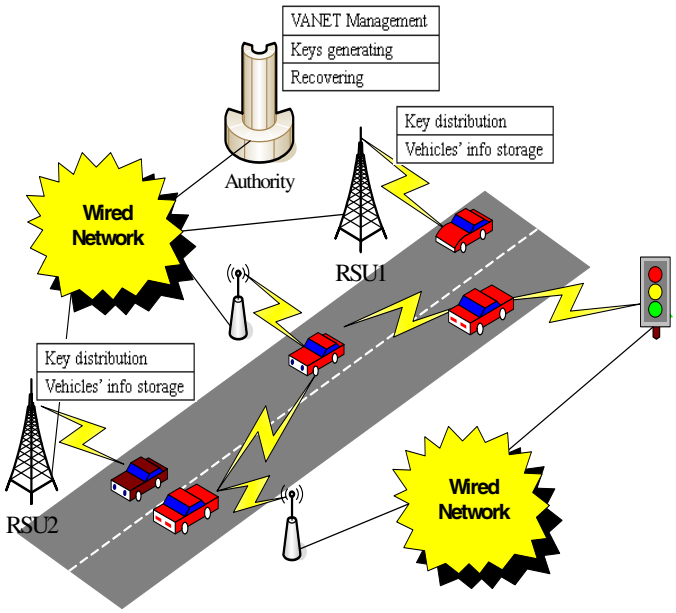

Fig. 1. The Architecture of a vehicular ad hoc network

C. Security Model

In this paper, we assume that attackers are inside, rational, active and global [12]. Inside attackers are legitimate members of the VANET. In this paper, attackers can be network nodes or road side infrastructure. Rational attackers only attack for their own benefits. They know the security mechanism and they want to attack without being detected. If there is a mechanism that can detect them, they tend not to attack if the punishment is severe enough. Active attackers have the ability to send packets into wireless channels. Global attackers have an unlimited scope in the network which means they can hear any information in the network.

We assume that the majority of vehicles and RSUs are honest and vehicles will report to the authority when they find that a vehicle is sending false messages. We also assume that wired network transmits data in secure without packets loss. Our protocol is used to judge whether a vehicle is a legitimate user. If accusers and accused are all legitimate users, we assume the authority has an evaluation system to judge the malicious [17]. The evaluation system design is out of the scope of this paper.

III. Security Protocol Design

A. Group Signature Scheme

We adopt short group signature [16] in this paper because it has smaller communication overheads than other group signature schemes. Meanwhile, in the short group signature protocol, there is a group private generator which can be

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

assigned to key distributors without revealing other secrets. The existence of the generator makes the third party possible to be key distributors. Another attractive feature of the short group signature is that it has a tracing key which can retrieve group private keys from signatures. The short group signature works as following[14]:

1) Key Setup: Let G_1 and G_2 be two bilinear multiplicative groups with generators g_1 and g_2 of the same prime order p, respectively. Let ψ be a computable isomorphism [13] from G_2 to G_1 with $\psi(g_2) = g_1$. Select $h \leftarrow G_1 \backslash \{1_{G_1}\}$ and ξ_1, ξ_2, $\gamma \leftarrow Z_p^*$ randomly and set μ, $\nu \in G_1$, such that $\mu^{\xi_1} = \nu^{\xi_2} = h$. Set $\omega = g_2^{\gamma}$. The group tracing key $K_t = (\xi_1, \xi_2)$. The group public key is (g_1, g_2, μ, ν, h, ω) and the group private key generator is γ.

2) Membership Registration: When a user k applies to join the group, the key distributor will select $x_k \leftarrow Z_p^*$ randomly and then sets $A_k = g_1^{1/(\gamma + x_k)}$. The group private key for the user k is $G_{pri_k} = (A_k, x_k)$. Then the key distributor securely transmits the group private key G_{pri_k} to the user K after it receives the valid information of the user. Each group private key should only be assigned to one user.

In our group signature scheme, vehicles are users. RSUs are key distributors and the authority is the tracer and the judge. The authority with responsibility of generating all the secrets holds group tracing key. The RSU in a group holds group private key generator. The vehicle gets group private key dynamically when it reaches an area that is controlled by an RSU. If there is a dispute in following procedures, the signature will be reported to the authority. The authority uses tracing key K_t and the signature to retrieve vehicle's group private key. If the authority gets the group private key, we can identify the vehicle because each group private key is only assigned to one user.

B. Protocol Design

In this section, we propose a protocol which is used to detect whether vehicles are using their own group private keys. It allows vehicles to be authenticated with their real identifiers under protection and guarantees the authority to find real identifiers of accusers and accused if there is a dispute. Our protocol consists of three steps: registration, message broadcasting and accusation. The authority makes decisions according to the registration information that vehicles provide. Consequently the registration procedure is the most important part in our protocol.

We assume that each vehicle and RSU is preloaded with a global, long term public/private key pair and a corresponding certificate of the public key signed by the Certification Authority(CA). We define the pair as Identity keys (*I-keys*). The group public key and group private keys are local, short term keys in our scheme. We define them as Group keys (*G-keys*). Both I-keys and G-keys are unique. So they are considered as identifiers of vehicles and RSUs. The authority also assigns an unique ID, like license plate number, to each vehicle. So each vehicle has two unique identifiers in our design. CA's public key is known by all vehicles. Furthermore, a hash function h(x)

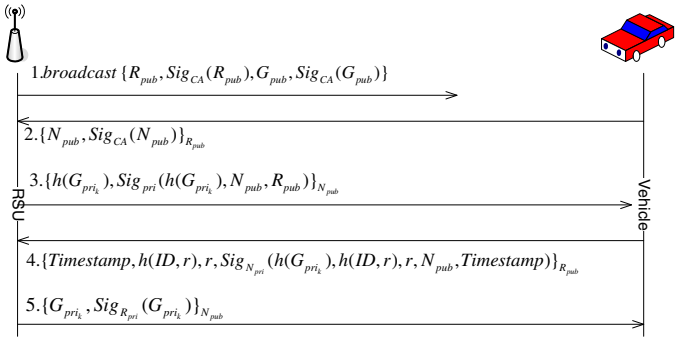

Fig. 2. Registration message flow.

TABLE I
NOTATIONS AND DESCRIPTIONS

R_{pub}/R_{pri}	RSU's public/private key pair (I-key)
N_{pub}/N_{pri}	Node(Vehicle)'s public/private key pair (I-key)
$Sig_A(M)$	Signature of message M signed by A or A's private key
M_k	Message M is encrypted by k or k's public key
G_{pub_k}/G_{pri_k}	Group public/private key pair (G-key) for user k
ID	The identifier of a vehicle
r	A random number which will be changed each time

is known by the authority, RSUs and all vehicles. It is used to provide the commitment in our protocol design. We assume that data are transmitted over TCP in wireless channels.

1) Registration: The procedure of registration is shown in Fig. 2. In Table I, we list physical meanings of symbols.

Message 1: RSU broadcasts its I-public key, G-public key and corresponding certificates regularly.

Message 2: When a vehicle detects RSU's hello message, it starts registration by sending its I-public key and the corresponding certificate to the RSU. Normally, a public key should not be encrypted. However, in our system model, each vehicle's I-public key is unique in the VANET, so it is also a identifier of the vehicle. We encrypt vehicle's I-public key to protect vehicle's privacy.

Message 3: The RSU sends the hash value of the G-private key which plans to be assigned to the vehicle and the signature of the hash value, vehicle's I-public key and RSU's I-public key to the vehicle. We need to emphasize that, in our protocol, RSU's I-public key is also unique. The vehicle can identify that the RSU is legitimate after it verifies this message because the RSU uses its I-private key in the message.

Message 4: The vehicle sends a random number, the hash value of its ID and the random number, the timestamp and the signature of corresponding information, shown in Fig. 2 message 4, to the RSU. The vehicle sends the hash value of its ID and a random number to the RSU as a commitment. We will use it to detect illegitimate users later. Meanwhile, the signature which is signed by the vehicle binds vehicle's information and the G-private key together. Then, the RSU can not re-map them because the RSU does not have vehicle's I-private key.

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

TABLE II
A REGISTRATION RECORD STORED IN THE RSU

$gpri_k$	N_{pub}	h(ID,r)	r	Timestamp	Signature

TABLE III
MESSAGE FORMAT FOR BROADCASTING

Grp ID	Msg ID	Payload	Time	$(ID, r)_{CA}$	r	Signature

Message 5: The RSU sends the G-private key to the vehicle after it gets message 4.

The vehicle finishes registration procedure after it gets a valid G-private key. At the same time, the RSU stores the information, as shown in table II, in the local database. The signature in the sixth item is the signature that the RSU receives in message 4. If the authority needs the information of a vehicle when there is a dispute, the RSU has to send the vehicle's corresponding information to the authority.

2) Messages Broadcasting: Vehicles can broadcast messages in the name of the group after they get G-private keys from the RSU. In this section, we present the message format for broadcasting. In our message format, as shown in Table III, group ID and message ID are used to identify groups and messages. Time means the timestamp. We add an encrypted ID in the message. Because it is encrypted by CA's public key, so it only can be known by the authority. The vehicle signs first six items in this message by using vehicle's G-private key, then we get the signature item. According to [15], the payload of a message is 100 bytes and the corresponding length of signature is 192 bytes.

3) Accusation: When a vehicle finds that other vehicles send false messages, it will report to the authority. For example, in order to travel faster, a vehicle may claim a traffic jam at a certain place. Other vehicles at that place should report the false message. The accusation message format is shown in Table IV. In the table, Msg means the message that a vehicle considers as false. G_{pub} is the G-public key that the accused and the accuser use. $(ID, r)_{CA}$ is accuser's ID encrypted with a random number by authority's public key. The accuser signs first five items in this message by using its G-private key.

After receiving an accusation, the authority verifies the signature in the accusation message by using G_{pub}. Then, the authority implements the open operations to get the accuser's and the accused's G-private keys if the signature is verified. Whereafter, the authority contacts RSUs which assign G-private keys to the accuser and the accused according to G-public keys. RSUs will send corresponding information back to the authority after they receive the requests from the authority. After that, the authority will calculate accuser's and accused's h(ID,r) by using IDs and random numbers which are got from the accusation message and the broadcast message respectively. If the value that the authority calculates is the same with the value it gets from the report, the user will be considered as legitimate. If both of them are authorized users, the authority will start the evaluation mechanism to decide

TABLE IV
MESSAGE FORMAT FOR ACCUSATION

Msg	Reasons	G_{pub}	$(ID, r)_{CA}$	r	Signature

which user tells the truth. The work flow of the accusation procedure is shown in the Fig. 3.

In our protocol, we only analyze accusations because we assume that vehicles will report messages which they consider as false. If nobody thinks a message is false, we do not need to know whether the sender is using its own group private key.

IV. PERFORMANCE ANALYSIS

The protocol that we design can defend compromised RSUs' attack. In this section, we present some possible attacks and explain the corresponding defence based on our protocol.

A. Appropriating the ID of other vehicles

In this attack, the compromised RSU may reply another vehicle's information to the authority if it finds that the investigated vehicle is its accomplice in the accusation procedure. Then, the malicious vehicle is protected and a well behaved vehicle is framed up.

In message 4, each vehicle has to sign its unique I-public key, hash value of G-private key and other information by using its own I-private key. Then, the vehicle's I-public key and its assigned G-private keys are bound together. RSUs can not re-map vehicles' unique I-public keys and G-private keys arbitrarily because RSUs do not have vehicles' I-private keys.

B. Receiving key without acknowledgement

In this attack, vehicles may not send message 4 to the RSU if the RSU transmits group private keys to vehicles before it receives message 4. Or sometimes messages may be lost in wireless channels. Without the signature in message 4, RSUs can not prove the relationship of a vehicle's I-public key and corresponding assigned G-private key to the authority. If this is the case, a compromised RSU will have an excuse to refuse to provide a malicious vehicle's information to the authority by replying that it did not get the signature at all.

In our design, the RSU only sends a commitment to the vehicle in message 3. The commitment is the hash value of G-private key and the signature of the hash value, RSU's I-public key and vehicle's I-public key. Then the vehicle have to submit a signature including its I-public key and the hash value of G-private key to the RSU, shown in message 4. The RSU will send the G-private key to the vehicle only after the it receives the verified signature in message 4. If the RSU does not send message 5 after it gets the vehicle's information, the vehicle has a commitment in message 3. It can report to the authority by submitting the commitment and related personal information. While it is also possible that the RSU sends the group private key to the vehicle but the vehicle claims that it does not get it. For example, maybe because of the packets loss in wireless channels. For vehicles and RSUs, both of them are possible to be malicious. But, RSUs are semi-trust which

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

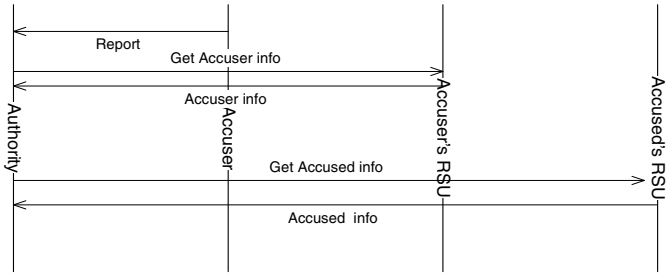

Fig. 3. Accusation message flow.

are more reliable than vehicles. So we let RSUs be the one who transmits critical information later.

As discussed above, an RSU must get message 4 before it assigns the G-private key, so it will be easy to detect that the RSU has been compromised if it can not provide the record for a G-private key.

C. Colluding with vehicles

In this attack, an RSU may collude with a malicious vehicle by sending other vehicle's G-private key to its accomplice. Then, the malicious vehicle can broadcast messages on behalf of other vehicles.

In message 4, the vehicle sends a commitment to the RSU which is a hash value of vehicle's real identifier and a random number. In every message that a vehicle broadcasts, its real identifier should be included in the message. If there is a dispute, the authority gets vehicle's information from the RSU. Then, it will calculate accuser's and accused's hash values by using vehicles' IDs and random numbers. If values that the authority calculates are the same as hash values reported by RSUs, the authority accepts the message. The malicious vehicle has no access to the corresponding ID of other vehicle's G-private key because the compromised RSU does not know it either. Hence, it's impossible for a malicious vehicle to attack.

Another attack is a malicious vehicle plans to frame up a normal RSU. It just needs to fill a wrong ID into the message. When the authority finds the mismatch, it will think there may be something wrong with the RSU.

The authority can not decide which is the malicious, the RSU or the vehicle or both, when it finds a mismatch of hash values. But the authority can be sure that, at least, there is one malicious between them. If the authority goes to check the RSU physically and finds that the RSU is working well, it can decide that the vehicle is a malicious one. As we discussed in the security model, attackers are rational. Malicious vehicles know that this kind of attack will be detected by the authority, so they tend not to attack in this way if the punishment is severe enough.

D. Deny of reporting

In this attack, the RSU may stop forwarding reports when an RSU colludes with a malicious vehicle.

This problem can be simply solved by reporting for several times because the possibility for an RSU to be compromised is low. As shown in Fig. 1, some RSUs which are in charge of the group private key distribution are key RSUs, such as RSU1 and RSU2. Other RSUs can forward reports to the authority although they do not have ability to distribute keys.

V. Conclusion

In this paper, we propose a novel distributed key management scheme for group signature based VANETs. In our network model, RSUs are key distributors. However, RSUs are semi-trust devices which may be compromised. Compromised RSUs may even collude with malicious vehicles. We design a security protocol to prevent compromised RSUs and malicious vehicles from attacking. Our design guarantees that RSUs distribute keys fairly and provide some mechanisms to detect compromised RSUs and malicious vehicles. In this paper, we only consider the case that an RSU handles a single group. The multi-group scenario will be studied in our future work.

References

[1] "SAFESPOT: Cooperative vehicles and road infrastructure for road safety," in http://www.safespot-eu.org/pages/page.php.

[2] "California Partners for Advanced Tansit and Highways," http://www.path.berkeley.edu/.

[3] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in *Proc. of PET*, pages 197-209, 2005.

[4] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real," in *Proc. of VTC*, April, 2007.

[5] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J.P.Hubaux., "Mix Zones for Location Privacy in Vehicular Networks," in *The First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 2007)*, in conjunction with QShine 2007, Vancouver, British Columbia, August 14, 2007.

[6] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1187-1192, 2005.

[7] K. Sampigethava, L. Huang, M.Li, R.Poovendran, K. Matsuura, K.Sezaki, "CARAVAN: Providing Location Privacy for VANET," in *Proc. of the 3rd international workshop on Vehicular ad hoc networks*, 2006

[8] D. Chaum and E. van heyst, "Group signatures," in *Proceedings of Eurocrypt 1991*, vol. 547, pp. 257-265, 1991.

[9] J. Guo, J.P. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," in *Proc. of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska, May 2007

[10] X. Lin, X. Sun, P.H. Ho and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications," in *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007

[11] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET," in *The Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007), in conjunction with ACM MobiCom 2007*, pp. 19-28, QC, Canada, September 2007

[12] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *the Workshop on Security in Ad hoc and Sensor Networks*, 2005.

[13] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography," CRC Press, ISBN: 0-8493-8523-7, October 1996.

[14] X. Sun, X. Lin, and P.-H. Ho, "Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme," in *Proc. of International Conference on Communications*, Scotland, June, 2007.

[15] U.S. Department of Transportation, "National highway traffic safety administration," in *Vehicle Safety Communications Project, Final Report*, Appendix H: WAVE/DSRC Security, April 2006.

[16] D, Boneh, X. Boyen, and Hovav Shamcham, "Short group signatures," in *Proc. of Advances in Cryptography - Crypto' 04, ser. LNCS*, vol.3152, Springer-Verlag, pp. 41-55, 2004.

[17] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *EPFL Technical report LCA-REPORT-2007-003*, 2007

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.