A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework

Jinhua Guo, John P. Baugh, and Shengquan Wang,

Published in CD-ROM *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska, May 2007

A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework

Jinhua Guo, John P. Baugh, and Shengquan Wang
Department of Computer and Information Science, University of Michigan-Dearborn
{jinhua, jpbaugh, shqwang}@umich.edu

***Abstract*— We propose a novel group signature based security framework for vehicular communications. Compared to the traditional digital signature scheme, the new scheme achieves authenticity, data integrity, anonymity, and accountability at the same time. Furthermore, we describe a scalable role-based access control approach for vehicular networks. Finally, we present a probabilistic signature verification scheme that can efficiently detect the tampered messages or the messages from an unauthorized node.**

***Index Terms*—group signature, probabilistic verification, security and privacy, VANET, vehicular networks**

I. Introduction

With emerging standards such as Dedicated Short-Range Communication (DSRC) [5] designated for vehicle-to-vehicle and roadside-to-vehicle communications, vehicles will soon be able to talk to one another as well as to their environment. By offering real-time traffic information, collision-avoidance assistance, automatic emergency incident notification, or vision enhancement systems, vehicular communications will help drivers make better informed, more coordinated, and more intelligent decisions, increasing the overall safety and efficiency of the national highway system.

Securing vehicular communications is an indispensable prerequisite for their deployment. Systems must ensure that the transmission comes from a trusted source and has not been tampered with since transmission. For example, with the Traffic Signal Violation Warning application [13], the in-vehicle system will use information communicated from the infrastructure located at traffic lights to determine if a warning should be given to the driver. An incorrect transmission from an invalid or compromised unit might jeopardize the safety of the vehicle and endanger others in the vicinity. Similarly, future implementation of safety applications, such as the Approaching Emergency Vehicle Warning application [13], would be greatly compromised without assurance that transmissions are from an actual emergency vehicle.

Privacy is another major issue. Vehicle safety communication applications broadcast messages about a vehicle's current location, speed and heading several times per second. With great potential benefits for safety and efficiency, however, comes great concern over how the enabling technologies will be used. For example, law enforcement could issue automatic speeding tickets. It would even be possible for malicious entities to track individuals, gather information and subsequently blackmail them with gathered information. There is a strong desire to provide user privacy so that the full identity of the vehicle sending each message is kept private. People who are concerned about tracking might disable their radio, impacting the safety and other benefits. The system also needs to reassure people that Big Brother is not in the passenger's seat.

Ensuring the security and privacy of vehicular wireless communications is still a formidable challenge. Conflicting goals such as security and efficiency as well as privacy and authenticity must be taken into account. Much of the previous literature, such as [12] and [10], has recommended use of traditional digital signature scheme. The major problem associated with traditional digital signature schemes is that in order to ensure privacy, the vehicles would have to store a very large number of public/private key pairs, and keys must be changed often. Secure distribution of keys, key management, and storage are very difficult in this type of scheme.

In this paper, we present a Secure and Privacy-Preserving Vehicular Communication framework. We propose a novel group signature based security scheme which relies on tamper resistance devices (requiring password access) for preventing adversarial attacks on vehicular networks. Compared to the traditional signature scheme, the new scheme achieves authenticity, data integrity, anonymity, and accountability at the same time. A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member, which effectively prevents a user from being tracked.

II. Related work

A. Security and Privacy in Vehicular Networks

Security and privacy are still open problems in vehicular networks. Contributions to security in VANETs have been general analyses, such as [7], [8], [9], [11], and [14].

Golle et al. introduced a scheme to detect malicious data in VANET [6]. It correlates data from different cars and cross-validate it against a set of rules. If most cars are honest, fraudulent data from a malicious car can be detected and then discarded. However, this approach relies on that the same event is observed by multiple entities, which is often not true. It is important to note that this approach is interesting particularly because it addresses insider attacks and is not primarily focused on authentication but on correctness of data.

Raya and Hubaux suggested a security and privacy scheme based on digital signatures under the PKI [11]. Each vehicle will be assigned a set of public/private key pairs. Each message sent will contain a digital signature and a corresponding certificate. Thus, the resulting total message might be three times the original message. To ensure privacy, a vehicle will have to store a large key/certificate set and frequently change keys. A vehicle should change its anonymous key within an interval of around one minute to avoid being tracked. Thus, if we assume that an average driver uses his car 2 hours per day, the number of required keys per year is approximately 43800, which amounts to around 21Mbytes. The secure distribution and storage of keys in this type of scheme remains an incredibly difficult challenge.

The most prominent industrial effort is carried out by the IEEE P1609.2 (Standard for WAVE - Security Services for Applications and Management Messages) Working Group. However, the Trial-Use IEEE P1609.2 standard [10], approved on June 8th, 2006, only provides mechanisms to authenticate WAVE management and application messages that do not require anonymity. It does not address the important and challenging security and privacy issues for the anonymous broadcast applications, pushing it to later phases of development.

B. Group Signatures

A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of a later dispute, open signatures, i.e., reveal the identity of the signer.

Group signatures were first proposed by Chaum and van Heyst [4]. However, the original schemes required that the group signature be linear to the size of the group. Recently, many improved schemes have been proposed with the signature size independent of the size of the group. The currently most efficient scheme that is secure under strong RSA assumption and the Difie-Hellman decision assumption is [3]. The short group signature [2] is more efficient; however it is based upon both Strong Diffie-Hellman and Linear assumptions. It utilizes signatures of lengths under 200 bytes, and offers about the same amount of security as an RSA signature of the same length.

III. Secure and Privacy-Preserving Vehicular Communication Framework

We propose a novel approach to securing vehicular networks while maintaining privacy. Our approach utilizes a group signature scheme, in which members maintain only a small number of secret key/group public key pairs. This scheme provides privacy due to the fact that signers are anonymous within the group from which they sign. Additionally, not only are signers anonymous within their group, but two messages signed by the same individual are not linkable, that is to say, one cannot determine if two messages came from the same member of the group, or two different members of the group. Our scheme achieves authenticity, data integrity, anonymity, and accountability simultaneously.

As an example of how integrity and authenticity are realized, consider a situation in which an emergency vehicle is approaching vehicles in a particular area. The emergency vehicle sends out an *approaching emergency vehicle warning* (AEV warning), which alerts all users in the vicinity. By using the group public key of emergency vehicles, all vehicles receiving the warning may verify that the message was indeed sent by an emergency vehicle. However, the emergency vehicle, say a police car, can maintain anonymity within its group.

Although it does make sense to maintain privacy of emergency vehicles, it is arguably more important for the privacy of civilian vehicles to be maintained. Thus, in the same manner, civilian vehicles organized in a region- and role- based access control system with group hierarchy (described later) will be able to maintain their anonymity within their own group. For example, a civilian vehicle may be identified by their group signature only as being from the Michigan/Southeast/Personal group. Thus they are indistinguishable from other members of the Michigan/Southeast/Personal group (that is, without the secret trapdoor knowledge of the group manager).

A. Why Group Signature?

Group signatures address the privacy issue by providing anonymity within a specific set of users, namely, a *group*. Groups consist of several members and one group manager (GM). A group signature is produced using the message to be signed (M), the secret signing key of the individual signing the message (*sk*), and the group public key (*gpk*).

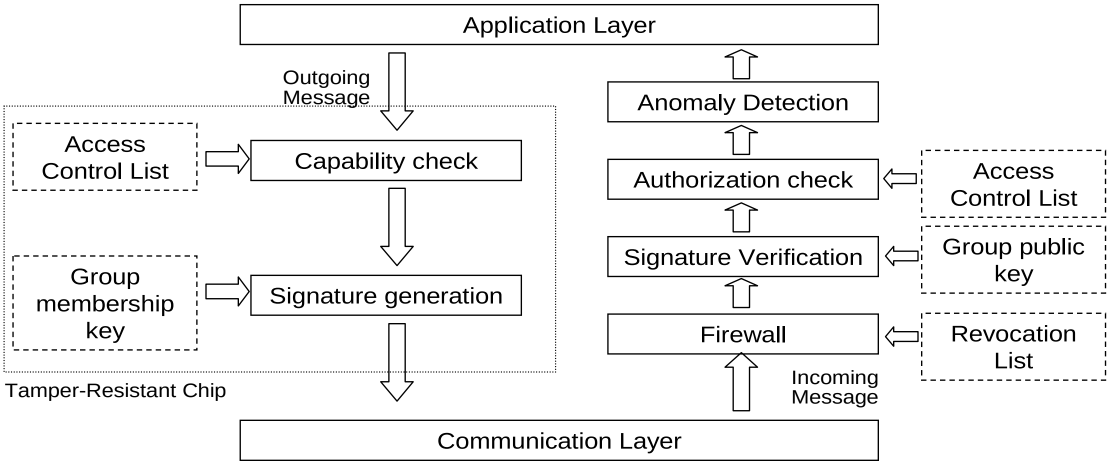

Fig.1 Secure and Privacy-Preserving Communication Framework

The privacy that group signatures provide is in the ability of any member of the group to sign a message on behalf of the group. The resulting message is verifiable as coming from a particular group, but the identity of the individual who signed the message is kept secret.

Additionally, to provide *accountability*, a message may be traced to the unique individual only by the group manager (GM) using its group manager secret key (*gmsk*). In general, the identities of individuals who sign various messages are kept secret. But, in the case of a dispute the GM may use its *gmsk* to essentially unlock the identity of the user. Otherwise, it should be computationally infeasible for an individual who is not the group manager to determine the identity of a specific group member without the *gmsk*.

Other qualities of group signatures are desirable, such as those in [1]. For example, *unlinkability* means that when a member signs multiple messages, the resulting signatures should not be linkable, that is, display characteristics that expose that they came from the same signer. This quality is based upon anonymity. If signatures are linkable, then the anonymity of the signer is reduced.

The *exculpability* quality of a group signature scheme means that no one should be able to sign a message and make it appear as if it came from a different member of the group. To provide clarification of this quality, if a group manager utilized his/her ability to open the message and determine the identity of a member, the resulting identity should reveal the actual individual of the signer, and not be forgeable.

Another quality pertaining to forgery is *unforgeability*. This quality is similar to exculpability, but pertains to forgery produced from outside the group. No one outside the group should be able to forge signatures and make them appear as if they came from the group. Thus, the distinction between exculpability and unforgeability is that exculpability can be seen as prevention of insider threats, while unforgeability can be seen as a prevention of outsider threats.

Coalition-resistance is yet another desirable property of group signatures. If some subset of the group (proper subset or even the entire group) colludes, they cannot create a valid group signature that the GM cannot attribute to one of the members in the colluding subset.

In the context of vehicular ad hoc networks, group signatures provide several desirable characteristics. In addition to the privacy provided by group signatures, scalability is also achieved due to the fact that vehicles would not need to maintain a public key for each user on the road with which it is likely to interact and instead maintains the group public key. This drastically reduces the number of keys to maintain.

Furthermore, the provision of special privileges to specific groups might be desirable. For example, emergency vehicles could be recognized by the infrastructure and the traffic signals might change in their favor.

Group signatures schemes must consist of at least five algorithms in order to be effective, including Setup, Join, Verify, Sign, and Open. The Setup procedure initializes the group public key, the group manager secret key, and other basic data about the group. The Join procedure allows new members to join the group. The Verify procedure utilizes the group public key and a message, and it determines whether or not a message originated from a particular group. The Sign procedure uses an individual member's secret signing key to sign a message. Finally, the Open procedure is used when the GM needs to determine the identity of a member who signed a particular message, providing traceability of the unique individual's identity, and subsequently, accountability.

B. Group-Signature Based Communication Framework

Utilizing group signatures as a foundation, we propose a new framework for establishing security and privacy. We require that all access to the system be authenticated. This access control will be enforced by a trusted tamper-resistant module located in the onboard system of the vehicle. In addition to these security features, privacy is maintained utilizing group signatures as a foundation for anonymous message signing. However, this privacy has an accountability quality to it. In the case in which false or compromised messages are sent, or in the case when liability must be determined, the group manager will be able to open messages for legitimate purposes, such as to determine the true identities of individuals involved with malicious data transfer.

This scheme simultaneously achieves authenticity, data integrity, anonymity, and accountability - all desirable characteristics for all honest and legitimate users involved, and for individuals as well as law and policy enforcement.

As shown in Fig.1, there are six fundamental components of the security layer of our framework. These six components are formalized as follows: *capability check, signature generation, firewall, signature verification, authorization check, and anomaly detection.*

First, the capability check serves as a first line of defense against malicious activity. The messages are checked and it is determined whether or not the sender is authorized to send a particular type of message, and checked against an access control list. If the sender does not have the right to send a particular type of message, that message will be dropped by the tamper-resistant module and will not be allowed to be broadcast through the network.

Second, an individual generates a signature utilizing a message M, and his/her group member secret signing key, *gmsk*.

Third, an incoming message first passes through a firewall which blocks unsigned messages and messages that are signed by vehicles in the Revocation List (RL). This firewall serves to prevent large-scale attacks such as viruses, worms, and DoS attacks.

Fourth, signature verification is performed on incoming messages. These messages have their signatures checked to determine what group the signer is a member of. Verification is done utilizing the group public key (gpk).

Fifth, an authorization check is performed after the group is determined to ascertain whether or not the signer had the right to send out the particular message. In the above example involving an emergency vehicle, an AEV warning message was broadcast. This alerts vehicles in the vicinity of the sender to its approach. In legitimate situations, the sender is a member of the emergency vehicle group. If the authorization check determines that the individual is not a member of the emergency vehicle group, then the message will be ignored.

Finally, the anomaly detection checks if the message received is consistent with the vehicle's own perception and messages received from other sources, as described in [6]. If not, it will drop the message and report the problem to the central authority. This is mainly to prevent malicious data attacks from insiders. If a problem is reported, a judge can order the disclosure of the true identity of the sender. This is possible since each message is uniquely signed and can be opened by the group managers (the identity disclosure capability should be distributed among multiple authorities). This will allow us to apply real world consequences (e.g. legal or financial) for misbehavior.

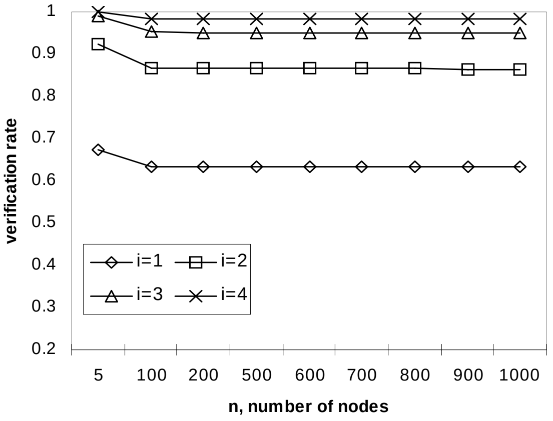

Fig. 2 The percentage of messages whose signatures are verified by at least one node

C. *Probabilistic Verification of Group Signatures*

Efficiency is a primary consideration and data must be delivered quickly in a vehicular environment. This is especially true of safety applications in which a matter of seconds or even milliseconds can mean the difference between life and death.

Group signatures are much less efficient than regular signatures. For example, the initial performance evaluation shows that it takes about 40ms to sign and 250ms to verify a message using the short group signature scheme [2]. We expect the performance of group signature could be significantly improved (e.g. pre-calculate all bases for exponentiation and fine tune the implementation). A vehicle typically needs to send several messages per second to inform its state to its neighboring vehicles, however, it may potentially receive hundreds or even thousands messages every second in dense networks. It is still very challenging to verify signatures of such a large number of received messages in a second.

We propose to probabilistically verify the signatures of received messages. In fact, it is not necessary to verify the signatures of all received messages. A broadcast message sent by a vehicle will be received by all vehicles within its radio range. If just one receiver verifies the signature, a tampered message or a message from an unauthorized node can still be detected. Suppose there are *n* nodes within the communication range of one another, each node verifies any random *i* messages out of every *n* messages received, the percentage of messages whose signatures are verified by at least one node is $1-(1-i/n)^n$. As shown in Fig. 2, if for *i* equals 3 (a node randomly verifies constant 3 messages per n messages received), the probability that at least one node verifies the signature of a message is always over 95% in both dense and sparse networks (*n* equals 1 to 1000).

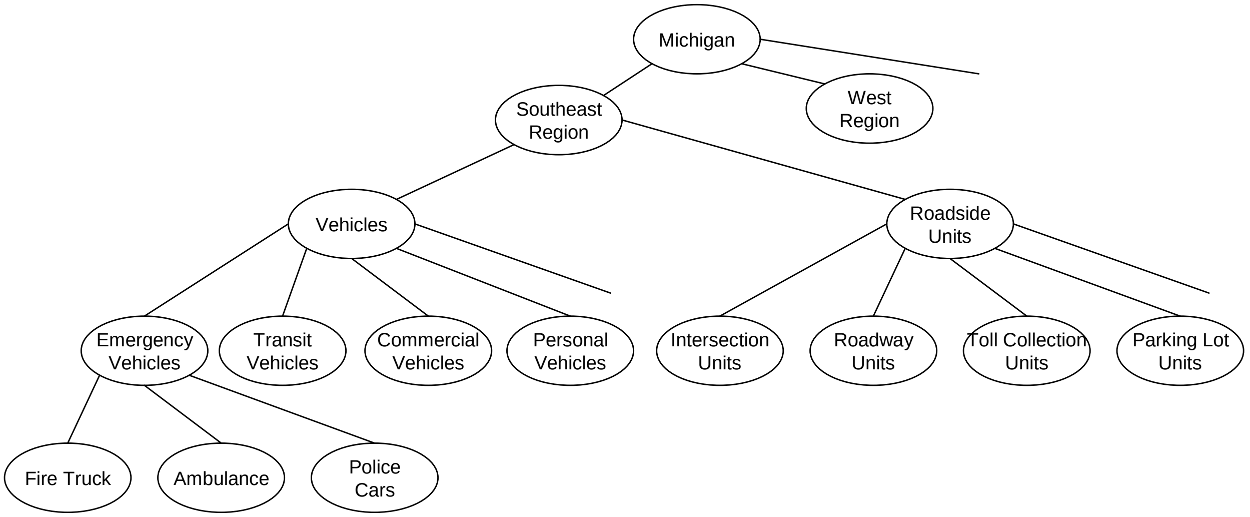

Fig. 3 Group Management

D. Group Management and Role-Based Access Control

In our scheme, we utilize a *regional and role-based access control* model. Vehicles, as well as roadside units (infrastructural units) will be classified based upon their region, and then by their specific role within the network.

Due to the incredibly large number of vehicles, it is essential to adopt a multi-level hierarchical structure. For example, as shown in Fig. 3, each state in the US could have a specific group. Within each state, a subgroup could belong to a specific region. Within each region, we will group vehicles as emergency vehicles, transit vehicles, commercial vehicles, maintenance and construction vehicles, and personal vehicles. In addition, we will group roadside units as intersection units, roadway units, toll collection unit, parking lot units, etc. Groups could also be further nested. For example, emergency vehicles can be further categorized into several subgroups, such as fire trucks, ambulance, and police cars. The nesting of groups enables the creation of hierarchical relationships that can be used to define inherited group membership and make each leaf group small enough.

To make access control more scalable, access rights to vehicular networks will be assigned to groups instead of individuals. Different groups may have different rights. For example, an *Approaching Emergency Vehicle Warning* message should only be issued by emergency vehicles. The controlled access to vehicular networks is enforced by an on-board trusted tamper-resisted device. A vehicle may belong to one or more groups. Since the number of groups is relatively small, all the relevant group public keys could be preloaded in the vehicles. There is no need to attach the group public key certificate with each message. This will reduce the message size and therefore improve the throughput.

One natural question that may arise from such a scheme is, "*What happens if an individual from one region enters another? Wouldn't there be diminished privacy?*". For example, wouldn't a vehicle from the southwest region of Michigan stick out if it were to travel, say to the northern region of New York? Although less efficient, one method of addressing this would be to provide all individuals with a separate group member secret key for each tier of the hierarchy to which he/she belongs. For example, one individual might have a national key, state key, region key, and role key. Then, depending upon which key the individual used, they could provide for themselves a larger anonymity set, with the tradeoff of diminished access rights.

E. Group Manager

A group manager is the individual that maintains a degree of authority over the group and is responsible for opening messages to retrieve the identity of individuals in cases where liability is in question. However, from the user's point of view, natural questions arise, such as, "*Who is the group manager?*", and "*Can I trust the group manager?*".

These are very valid questions, and must be carefully considered when designing groups and related policies. We suggest that the solution to the trustworthiness of the group manager is to distribute the ability to open messages. The Open procedure is the key element for accountability in group signature schemes that allows a group manager to determine the identity of an individual who sent a message. That is to say, the Open procedure is the procedure which has the potential to violate any group member's privacy if it is abused.

Thus, as the administration desires to keep general users in the network accountable for their actions, it is desirable for the users of the network for the group manager to be held accountable as well. As alluded to above, we suggest distribution of the ability to use the Open procedure. Thus, a natural way to do this is to provide several different entities with chunks of the group manager secret key. Thus, no single individual entity will maintain this key and be able to open signatures by itself. Therefore, the individual entities maintaining portions of the key must collude in order to open the message.

For example, a judicial entity (e.g., a court) could maintain a portion of the group manager secret key. Additionally, an executive entity, such as a presidential or gubernatorial entity, could maintain a second portion. Finally, a legislative entity such as a senate could maintain the third portion of the key. Thus, the natural checks and balances of our constitutional system could be applied to the group management system. Obviously, the exact organization of these entities' interaction with the Open procedure would necessitate committees or representatives of each of the three governmental units.

Regardless of the exact distribution of the key, it should be clear that this type of system is far better than a system in which a single entity has full control over the Open procedure.

F. Tamper-Resistant Devices for Key Storage

Keys stored inside a vehicle computer can be vulnerable to use, abuse, duplication, and modification by an unauthorized attacker. To protect keys, we will store them in a tamper-resistant hardware device. This device offers physical protection to the keys residing inside them, thereby providing assurance that these keys have not been maliciously read or modified. In addition, this device will also be responsible for verifying the access rights and signing outgoing messages.

The use of a tamper-resistant device allows preventing an *untrusted* member from cheating, by letting his *trusted* device both secretly store the signature keys and control their legitimate usage. The access to the contents of a tamper-resistant device requires knowledge of a PIN or password, will be restricted to authorized people. Group membership keys should be renewed periodically (for example, annually at the license plate renewal)

IV. CONCLUSIONS

The deployment of vehicular communication networks is rapidly approaching. There is an urgent need to develop techniques that ensure both security and privacy in vehicular networks. We introduce a novel group signature based security framework for vehicular communications. Compared to the traditional signature scheme, the new scheme achieves authenticity, data integrity, anonymity, and accountability at the same time. Furthermore, we present a probabilistic signature verification scheme that can efficiently detect the tampered messages or the messages from an unauthorized node.

Research into an optimal method of key distribution is needed. It is still unclear as to the best method of key distribution. Questions arise, such as, "should the key distribution occur at regular intervals with license renewal?", "should there be special times when the owners must go in and have their keys updated?" etc. However, special times to update keys would be an inconvenience for most owners, so the updates and distributions should perhaps be done during regular maintenance or license renewal. The question of key distribution is still a largely open topic in regard to vehicular ad hoc networks.

ACKNOWLEDGMENTS

This work is partially supported by NSF under the grant # CNS-0521142 and University of Michigan under an OVPR grant and a CEEP grant.

REFERENCES

[1] M. Bellare, Daniele Micciancio, Bogdan Warinschi, "Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions." *Advances in Cryptography Eurocrypt '93 Springer-Verlag*.

[2] D. Boneh, X. Boyen, H. Shacham, "Short Group Signatures," *CRYPTO 2004*.

[3] J. Camenisch and J. Groth, "Group signatures: Better efficiency and new theoretical aspects," *In Security in Communication Networks 2004*, volume 3352 of LNCS, Springer Verlag, 2005.

[4] D. Chaum, E. van Heyst, "Group Signatures," *Advances in Cryptology: EUROCRYPTO'* 1991.

[5] DSRC Consortium, http://www.leearstrong.com/dsrc/dsrchomeset.htm

[6] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," *in VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pp. 29–37.

[7] J. Guo and J. P. Baugh, ""Security and Privacy in Vehicle Safety Communication Applications," *2006 SAE Transactions: Journal of Passenger Cars - Electronic and Electrical Systems,* pp. 721-727.

[8] A. Held and R. Kroh, "It-security and privacy for Telematics services," *in Workshop on Requirements for Mobile Privacy & Security*, University of London, UK, September 2002.

[9] Jean-Pierre Hubaux, Srdjan Capkun and Jun Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security & Privacy Magazine*, 2(3), May 2004, pp 49--55.

[10] IEEE Std P1609.2 -2006 – IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. July 6, 2006.

[11] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," *Proc. of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.*

[12] M. Raya and J. Hubaux, "The Security of Vehicular Ad hoc Networks," *Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 2005*.

[13] Vehicle Safety Communications Consortium, "Vehicle Safety Communications Project Task 3 Final Report, Identify Intelligent Vehicle Safety Applications Enabled by DSRC," March 2005.

[14] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," *In European Wireless*, 2002.