This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks

Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada
{h9zhu, xdlin, rxlu, pinhan, xshen}@bbcr.uwaterloo.ca

***Abstract*— To achieve efficient authentication on emergency events in vehicular ad hoc networks, we introduce a novel aggregated emergency message authentication (AEMA) scheme to validate an emergency event. We make use of syntactic aggregation and cryptographic aggregation techniques to dramatically reduce the transmission cost, and adopt batch verification technique for efficient emergency messages verification. Compared with existing emergency message authentication approaches, our scheme shows the superiority on generality, enhanced security and efficiency.**

I. Introduction

As the advancement of telecommunications, Vehicular ad hoc Networks (VANETs) have attracted extensive attentions from both industry and academia, and are expected to serve as a killer application in the future Internet and telecommunication market. Such an application scenario allows communications between vehicles (or referred to Inter-Vehicle Communication (IVC)) as well as between vehicles and the infrastructure (or referred to Roadside unit (RSU) to Vehicle communication (RVC)), which are mainly positioned for ensuring traffic safety and driving experiences. For example, it can be used to alert drivers for potential traffic jams and provide increased convenience and efficiency. Among all of vehicle communication network applications, dissemination of emergency messages to the vehicles in a specific area is very crucial. The fast propagation of emergency and local warning messages to the approaching vehicles will be helpful for preventing secondary accidents. In most cases, a VANET carries out such an emergency message propagation in a multi-hop transmission manner, particularly in the suburban areas where less RSUs are installed.

Many previously reported studies have focused on data dissemination in VANETs [1], [2]. However, the security issues, especially on how to ensure the authenticity of emergency messages in a VANET, are still subject to a great challenge. Firstly, since most of the life critical applications in VANETs rely on multi-hop transmission to disseminate data packets to the surrounding geographical area, the hostile adversaries may intentionally forge an invalid emergency event, which may pose a serious threat on road safety. Secondly, in such a highly dynamic network environment with potentially a large number of vehicle nodes, the conventional security mechanisms, such as public key certificate and digital signature, are not sufficient to ensure the security of VANETs since the adversaries can still launch the attack by compromising one or several nodes and disseminate false emergency messages with the credentials of the other users. On the other hand, for a specific emergency event, it is expected that multiple sensing vehicles could detect the common event. As shown in Fig. 1, the sensing vehicles not only include the current witness vehicles (the yellow vehicles) but also potential witness vehicles (the white vehicles) which are approaching the emergency event promptly. Therefore, taking advantage of the common view of these sensing vehicles to cross-validate the emergency event could possibly serve a promising approach to enhance the overall security level in VANETs. Such a method of cross-checking the emergency event by collecting the feedback of witnesses is defined as *voting mechanism*, which is originally used to detect the misbehaving nodes in a distributed ad hoc network without any centralized security authority [3]. The mechanism can be migrated to VANETs to enhance the overall security of emergency events authentication [4], [5]. In [4], a voting scheme is implemented on location based groups, where vehicles are grouped according to their location. Within each group, a group leader will be elected to take the responsibility of collecting more than a threshold k of proofs from k distinct witnesses to prove the validity of an emergency event. However, such a group based voting mechanism certainly faces the challenge of highly dynamic network topology in VANET, which requires extra efforts to maintain the location based groups. In addition, in an area with low vehicle density, it can not be guaranteed that the group leader can collect more than k supporting signatures within the group. In [5], the concept of "voting" is further extended to the "destination voting" strategy. The witnesses will continuously generate the emergency reporting messages to the remote vehicles. The remote receivers will make a decision based on collected messages by checking if the majority of these messages are consistent.

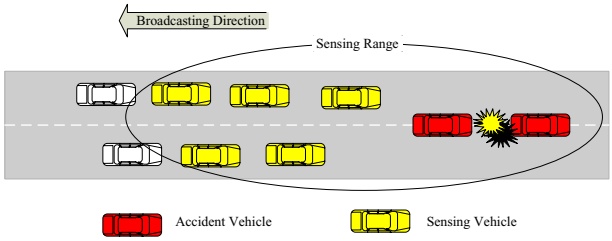

Fig. 1. Emergency Event Sensing in VANETs

The voting mechanism can effectively improve the security of VANET at the expense of increased computation and transmission overhead. For both approaches in [4], [5], to prevent

the attackers from sending duplicate emergency messages, only distinct messages from distinct vehicles are considered. Therefore, every emergency message will be signed by the sender in order for the receivers to authenticate. However, the size of digital signatures is typically very large in the order of tens (using Elliptic Curve Cryptography) to hundreds of bytes (RSA), which will incur more transmission overhead. Furthermore, generating and verifying a digital signature and its corresponding certificate will also incur additional computation cost. Such transmission and computation costs will be further scaled up with the number of active sensor vehicles. When all these vehicles transmit the information by way of flooding or geocasting, the transmission and computation overhead can easily overload the network. Therefore, aggregating the relevant emergency messages as well as providing messages authentication is of high importance.

In this paper, we propose a novel aggregated emergency message authentication (AEMA) scheme to efficiently validate the emergency messages in VANETs. The basic idea is that during the emergency messages opportunistic data forwarding process, a vehicle can hold multiple messages, which can be aggregated into a single one before the vehicle launches aggregated message in the air. The proposed AEMA scheme takes advantage of *syntactic and cryptographic aggregation technique* to reduce the transmission cost and adopt *batch verification* technique to reduce the computation cost [7]. We will demonstrate that the proposed scheme can dramatically reduce both computation and transmission overhead in achieving efficient authentication on emergency messages.

The remainder of the paper is organized as follows. In Section II, we present the system model, attack model, and the design goals. Section III gives a review on some preliminary background. In Section IV, the proposed AEMA scheme is presented in detail. Performance analysis is given in Section V, followed by the conclusion in Section VI.

II. System Model and Design Goal

This section describes our system model, attack model and design goals.

A. Network Model

We consider IVC in a VANET without any presence of fixed infrastructure such as access points, RSUs, and satellite communication for assisting data propagation. There are two types of entities in AEMA, namely the *Offline Security Manager (OSM)* and the vehicles. Before joining the network, every vehicle should register to the OSM and obtain its corresponding public key certificate. We assume an opportunistic data forwarding mechanism is adopted [1], [2], in order to achieve the globally routing objective.

B. Attack Model

In this study, we mainly consider the *false data injection attacks* where the goal of an attacker is to make the receiver vehicles to accept false emergency reports. To maximize the effectiveness of the attacks, multiple adversaries could collude to launch an attack by cooperatively injecting false messages, which is also known as a *collusion attack*. Similar to other distributed trust mechanisms, the number of adversaries in the system during a given time period, e.g., the public key revocation period, is less than a threshold denoted as k. Therefore, unless explicitly specified, an emergency event can be considered to be true at the receiver if and only if more than k signatures from k distinct witnesses are collected.

C. Design Goals

The proposed AEMA scheme has the following security and efficiency design goals:

- *Collusion Freedom*: No subset of k or less vehicles can forge an emergency event.
- *Efficient Authentication*: The proposed emergency message authentication scheme should be performed in an efficient way to reduce the communication and transmission overhead.
- *Generality*: The proposed scheme should be applicable in different network densities including both of high density and low density cases.

III. Preliminaries

A. Pairing Technique

The proposed AEMA scheme is based on bilinear pairing which is briefly introduced as below. Let $\mathbb{G}$ be a cyclic additive group and $\mathbb{G}_T$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}| = |\mathbb{G}_T| = q$. Let g be a generator of $\mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be an efficient admissible bilinear map with the following properties:

- Bilinear: for $a, b \in \mathbb{Z}_q^*$, $e(g^a, g^b) = e(g, g)^{ab}$.
- Non-degenerate: $e(g, g) \neq 1$.

B. Aggregate signature and Batch verification

The major computation cost for authenticating an emergency message comes from verifying a set of supporting signatures issued by different emergency witnesses. The corresponding public key certificates of the signers also need to be verified together. All of them will incur a significant amount of transmission and verification cost. In this study, we take advantage of aggregate signature to reduce the transmission cost of supporting signatures and certificates and batch verification to realize efficient signature verification.

An aggregate signature is a digital signature that supports aggregation of n distinct signatures issued by n distinct signers to a single short signature [6]. This single signature (and the n original messages) will convince the verifier that the n signers indeed sign the n original messages. In addition to enjoying the benefit of the reduced transmission size, aggregate signature technique supports batch verification, which enables the receivers to quickly verify a set of digital signatures on different messages by different signers. In this study, we adopt the aggregate signature and batch verification introduced in [7] as our basic cryptographic aggregation technique to improve the aggregation performance.

IV. AEMA PROTOCOL

We present the details of the five procedures of our AEMA protocol.

A. System Setup

The OSM generates a tuple $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ as the system parameters. The OSM selects a random $sk \in \mathbb{Z}_q^*$ as its secret key and generates its public key $pk = g^{sk}$, by which four hash functions are formed: $H : \{0,1\}^* \rightarrow \mathbb{G}$, $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q$. The group public key and secret keys are $(q, g, \mathbb{G}_1, \mathbb{G}_T, e, pk, , H, H_1, H_2, H_3)$ and sk, respectively.

An important task of the setup procedure is to determine the format of emergency report message. In our study, the format of a secure emergency report (SER) is defined as follows. For an emergency event $\mathcal{E}_i$, the sensor vehicle $\mathcal{V}_j$ will generate a SER_j^i:

$$SER_j^i = (Type_i, Loc_i, ID^j, Time_j^i, Sig_j^i, Cert_j) \quad (1)$$

where

$Type_i$— denotes the type of emergency event reported in this report.

Loc_i— denotes the place where the emergency event takes place.

ID_j— denotes the identity of the vehicle that generates the claim.

$Time_j^i$— denotes the time when the vehicle j makes the claim on this emergency event i.

Sig_j^i— denotes the supporting signature generated by vehicle j on emergency event i.

$Cert_j$— denotes the certificate held by vehicle j.

For a specific event $\mathcal{E}_i$, it is reasonable to assume that the revelent SERs will share the same $Type_i, Loc_i$.

B. Registration

A vehicle can join the network by performing the following steps:

1) **Public Key Generation** A vehicle can randomly choose $x_j \in \mathbb{Z}_q^*$ as its secret key and generate its public key $X_j = g^{x_j}$. To keep the identity privacy, the vehicle can also randomly choose $\mathcal{V}_j$ as its pseudonym. Before joining the VANET, $\mathcal{V}_j$ will contact the OSM to obtain its corresponding certificate.
2) **Public Key Certificates Issuing** After ensuring the legitimacy of this vehicle, the OSM will issue its public key certificate by signing its signature on $(\mathcal{V}_j, X_j)$. Here, the certificate generation process follows a typical Boneh, Lynn, and Shacham signature scheme in [6]. The OSM computes $h_j \leftarrow H(\mathcal{V}_j || X_j)$ and $\sigma_j \leftarrow h_j^{x_j}$. $Cert_j = (\mathcal{V}_j, X_j, \sigma_j)$ is the public key certificate of $\mathcal{V}_j$.
3) **Certificate Verification** Given a vehicle's public key certificate $Cert_j$, $h_j \leftarrow H(\mathcal{V}_j || X_j)$ can be computed, and it is accepted if $e(\sigma_j, g) = e(h_j, pk)$.

C. SER Generation and Broadcasting

Once an emergency event $\mathcal{E}_i$ is sensed by one or multiple vehicles and the observation is $(Type_i, Loc_i, Time_j^i)$, the sensing vehicles $\mathcal{V}_j, j = 1, 2, \ldots$ may independently generate their SERs as follows.

1) **SER Generation** Given the type and observation time of the emergency message $TL_i = Type_i || Time_j^i$ as well as the location information $\ell_i = Loc_i$, a witness vehicle with its public and private key pairs (X_j, x_j) can compute $w_i \leftarrow H_3(TL_i || \ell_i)$, $a \leftarrow H_1(\ell_i)$, $b \leftarrow H_2(\ell_i)$ and generate the signature $Sig_j^i = a^{x_j} b^{x_j w_i}$. Thus, $(Type_i, Loc_i, \mathcal{V}_j, Time_j^i, Sig_j^i, Cert_j)$ constitutes a SER claim generated by vehicle j toward event i. After that, $\mathcal{V}_j$ will broadcast this SER_j^i to its neighbors.
2) **SER Verification** A single SER verification can be performed as follows: given $SER_j^i = (Type_i, Loc_i, \mathcal{V}_j, Time_j^i, Sig_j^i, Cert_j)$, the verifier will first check the validity of certificate included in this SER. After that, it can check the validity of supporting signature by computing $w_i \leftarrow H_3(TL_i || \ell_i)$, $a \leftarrow H_1(\ell_i)$, $b \leftarrow H_2(\ell_i)$. It is accepted if $Sig_j^i = a^{x_j} b^{x_j w}$.

D. SER Opportunistic Forwarding

In VANETs, the network topology could be very dynamic and diversified in shape from time to time, even sometimes sparse and frequently partitioned, the communication between vehicles are expected to be performed in an opportunistic manner, where nodes carry packets when routes do not exist, and forward the packets to the new receiver that moves into its vicinity [1]. To enable the opportunistic data propagation, vehicles that are within a range r and maintain connectivity for a minimum time t with each other, can be arranged to form a cluster. The detailed discussion on cluster creation and maintenance can be found in [1]. We refer the node at the head of every cluster as header, which is responsible for forwarding the data to the next cluster in a typical opportunistic data forwarding algorithm such as [1], [2]. The messages will be buffered at the header until they are forwarded to the next cluster, which is also referred to as the "*Carry and forward*" strategy. In this study, it is considered that the header can also play the role of emergency message aggregator because of the following two reasons:

1) If taking a header of a cluster as the aggregator, the aggregation process will be merged into a part of data forwarding process. Therefore, there is no need to elect another cluster head to perform the data aggregation operations.
2) The process of message propagation between two clusters is referred to as a catch-up process, where a message traverses along with its carrying vehicles until it reaches within the radio range of the vehicle at the end of another cluster, which obviously presents a considerable propagation interval depending on the speed of vehicles and the gap between clusters. Therefore, we can use such

an interval to aggregate the related emergency messages to minimize the aggregation latency.

In the following sections, a cluster head will be taken as the aggregator of the cluster, which will perform the following SER aggregated authentication algorithm.

E. SER Aggregated Authentication

For any specific emergency event $\mathcal{E}_i$, each aggregator maintains two local message lists, which keep the forwarded SERs and ReadytoForward SERs, respectively. The forwarded message list, denoted as $\mathcal{F}$, contains all the SERs which have been forwarded by this vehicle before, while the ReadytoForward message list, denoted as $\mathcal{R}$, stores messages which have not been transmitted but can be forwarded some time later. The $SERs$ set $\mathcal{F} \bigcup \mathcal{R}$ include all the $SERs$ related to event i. Whenever receiving a SER, the aggregator should check if this SER is a duplicate. If yes, such a SER will be dropped, otherwise it will be put into the message list R. Before the forwarded propagation, the aggregator will perform the SER aggregation (or *Aggregate_SER*) and SER batch verification (*BatchVerify_SER*) operations as follows.

1) ***SER Aggregation****: Aggregate_SER* is used to aggregate multiple SERs into a single SER, which includes two steps: *syntactic aggregation* step and *cryptographic aggregation* step.

a) Syntactic aggregation: For emergency event i, given n SERs $SER_j^i = (Type_i, Loc_i, \mathcal{V}_j, Time_j^i, Sig_j^i, Cert_j)$ by vehicles $\mathcal{V}_j, j = 1, \ldots, n$, we can obtain syntactically aggregated SER as $SER_{agg} = (Type_i, Loc_i, \mathcal{V}_1, \ldots, \mathcal{V}_n, Time_1^i, \ldots, Time_n^i, Sig_1^i, \ldots, Sig_n^i, Cert_1, \ldots, Cert_n)$.

b) Cryptographic Aggregation: It is used to aggregate multiple signatures and certificates into a single signature and certificate, which includes the following two steps.

  a) Certificate Aggregation: $Cert_{agg} \leftarrow (\mathcal{V}_j, X_j, \sigma_{agg})$, where $\sigma_{agg} \leftarrow \prod_{j=1}^{n} Cert_j$.

  b) Signature Aggregation $Sig_{agg} \leftarrow \prod_{j=1}^{n} Sig_j^i$.

The above aggregation procedure is illustrated in Fig. 2. After syntactic aggregation and cryptographic aggregation, we can obtain the aggregated SER as $SER_{agg} = (Type_i, Loc_i, \mathcal{V}_1, \ldots, \mathcal{V}_n, Time_1^i, \ldots, Time_n^i, Sig_{agg}, Cert_{agg})$.

2) ***SER Batch Verification****: BatchVerify_SER* includes batch signature and certificate verification which are given as follows

a Certificate Batch Verification: Given a aggregated certificate $Cert_{agg} \leftarrow (\mathcal{V}_j, X_j, \sigma_{agg})$, the verifier accepts if $e(\prod_{j=1}^{n} \sigma_j, g) = e(\prod_{j=1}^{n} h_j, pk)$ holds.

b Signature Batch Verification: Given the aggregate signature Sig_{agg}, the message set $SER_i^j | \leq i \leq n$ and public keys $X_i | \leq i \leq n$ for all the vehicles in set $\mathcal{V}$, accept if $e(Sig_{agg}, g) = e(a, \prod_{i=1}^{n} X_i) \times e(b, \prod_{i=1}^{n} X_i^{w_i})$.

If the batch verification holds, the aggregator will accept SERs in list $\mathcal{R}$ as valid SERs. Then the aggregated SER in $\mathcal{R}$ will be forward-propagated. Meanwhile, the aggregator will put all the SERs in $\mathcal{R}$ to message list $\mathcal{F}$. Once the total number of

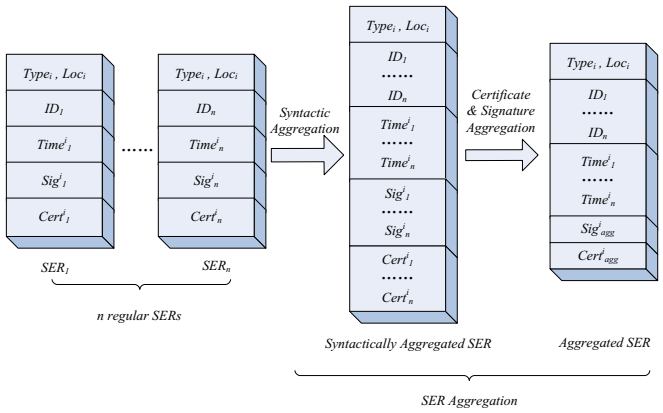

Fig. 2. SER Aggregation: Syntactic Aggregation and Cryptographic Aggregation

$\mathcal{F}$ exceeds k, this emergency event $\mathcal{E}_i$ will be accepted as a valid emergency event. The above algorithm is summarized in algorithm 1.

Data: **Input** $(\mathcal{F}, \mathcal{R}, SER')$
Result: **Output** `valid` or `invalid`

if $|\mathcal{F}|+|\mathcal{R}| < k$ **then**
  for *any newly received* SER' **do**
    if $SER' \notin \mathcal{F} \cup \mathcal{R}$ **then**
      Add_List($\mathcal{R}$*,* SER'*);*
    end
    else Drop SER' ;
  end
  SER_agg← *Aggregate_SER(*$\mathcal{R}$*);*
  if *BatchVerify_SER(*$\mathcal{R}$*)* **then**
    ForwardPropagation($\mathcal{R}$*)*;
    Add_List($\mathcal{F}$*,* $\mathcal{R}$*);*
  else
    return *invalid*;
  end
end
else
Accept emergency event as True ;
return `valid`;

Algorithm 1: SER Aggregated Authentication

V. Security Discussion

A. Collusion Attacks

The effectiveness of AEMA for defending against a collusion attack is based on the combination of the traceability property and the distributed trust mechanism. The traceability property ensures that any adversary sending multiple claims against a common event will be detected. As a result, an adversary can only send one SER per event. Moreover, the existence of the distributed trust mechanism guarantees that the number of adversaries in the VANET system is less than k. Consequently, even if all the adversaries collude with each

other, they cannot generate k or more SERS to convince the other vehicles the existence of a non-existent emergency event.

B. Privacy Protection of Witnesses

In AEMA, we propose to use randomly generated pseudonyms as well as corresponding public key certificates to preserve the privacy of witness vehicles. To further enhance the privacy preserving functionality of AEMA scheme, before joining the VANET, a vehicle can request multiple pseudonyms and corresponding public keys from OSM. To avoid Sybil attacks which are defined as a malicious vehicle impersonates multiple identities, we should carefully define the expiration date of public key certificates to ensure that only one pseudonym and public key certificate is valid for any time slot.

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed AEMA scheme in terms of the resultant communication cost and computation overhead. To demonstrate the superiority of AEMA, we also compare AEMA with the existing approach in [4], which adopts the non-aggregated ECDSA signature scheme as building blocks.

A. Transmission Cost

One of the major advantages of AEMA is the reduction of transmission cost. The communication cost is determined by the size of aggregated SERs, which is mainly due to the supporting signatures and corresponding public key certificates. To ensure the security of the protocol, the elements in $\mathbb{G}$ could be up to 160 bits for achieving a security level comparable with ECC-160. Since the signature and certificate in AEMA only require one element in $\mathbb{G}$, respectively, the whole supporting signature plus the certificate could be represented in three $\mathbb{G}$ elements, or 480 bits. The approximated length of components of a SER in AEMA is shown in Table I. If we take multiple SERs into consideration and the total number of the collected SERs is n, the total size of the SERs without aggregation should be $92n$. However, in our AEMA scheme, the total size can be reduced to $36n+56$ by taking advantage of aggregation signature, which is also shown in Table I. Under the same parameter assumption, the total size of concatenated ECDSA signatures scheme is 116n+36 in [4], which is much longer than that of the AEMA scheme.

TABLE I
THE SIZE OF EACH COMPONENT OF SER(BYTES)

Component	T& L	ID	Time	Sig	Cert	Total
Size	16	8	8	20	20+20	92
Aggregated	T& L	nID	nTime	Sig_{agg}	$Cert_{agg}$	Total
Size	16	8n	8n	20	20n+20	36n+56

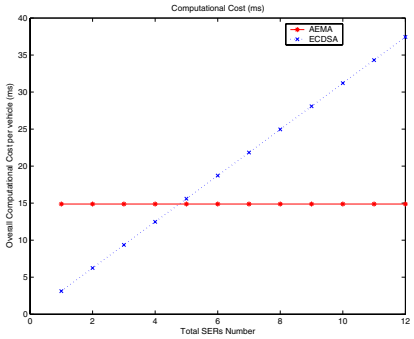

Fig. 3. Comparing AEMA with ECDSA based authentication scheme with different number of SERs

B. Computation Cost

The computation costs are measured by the most expensive pairing (Pair) and point multiplication (Pmul) operation. Because of the cryptographic aggregation technique, the aggregate verification cost on n distinct signatures and certificates costs about only 5 pairings, which is a significant improvement over the 3n pairings required by individual verification. As a comparison, ECDSA signature scheme requires $2n$ Pmul operation. By adopting the pairing technique in [8], we can obtain the rough time costs for Pair and Pmul to be 2.82 ms and 0.78 ms, respectively. From Fig. 3, we can observe that the computation cost of the AEMA scheme keeps constant even if the number of SERs increases; while the computation cost of ECDSA increases with the increase of SERs until significantly exceeding the computation costs of AEMA.

VII. Conclusions

In this paper, we have proposed an efficient aggregated emergency message authentication scheme, which can effectively address both of efficiency and security issues in VANETs. Our future research will integrate the aggregated authentication scheme with the data forwarding algorithm to achieve the best aggregation effect.

References

[1] T. D.C. Little and A. Agarwal, "An Information Propagation Scheme for VANETs," in Proc. of *IEEE Conference on Intelligent Transportation Systems*, Sep. 13-16, 2005.
[2] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "MDDV: A Mobility-Centric Data Dissemination algorithm for Vehicular Networks," in Proc. *1st ACM VANET*, 2004.
[3] X. Lin, H. Zhu, B. Lin, P.-H. Ho and X. Shen, "A Novel Voting Mechanism for Compromised Node Revocation in Wireless Ad Hoc Networks," in Proc. of *GLOBECOM'06*, San Francisco, Nov. 27-Dec. 1, 2006.
[4] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient Secure Aggregation in VANETs," in Proc. of *VANET'06*, 2006.
[5] B. Ostermaier, F. Dotzer, M. Strassberger, "Enhancing the Security of Local DangerWarnings in VANETs - A Simulative Analysis of Voting Schemes," in Proc. of *ARES 2007*, April 2007.
[6] D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing," in *Journal of Cryptology*, vol. 17, no. 4, pp. 297-319, 2004.
[7] J. Camenisch, S. Hohenberger and M. Pedersen, "Batch Verification of Short Signatures," in *Eurocrypt 2007*, pp. 246-263, 2007.
[8] P. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and Provably-Secure Identity-based Signatures and Signcryption from Bilinear Maps," in *AISACRYPT 2005*, pp. 515-532, 2005.