Anonymous Announcement System (AAS) for Electric Vehicle in VANETs

Man Ho Au[1], Joseph K. Liu[+2], Zhenfei Zhang[3], Willy Susilo[4], Jin Li[5] and Jianying Zhou[6]

[1]*Hong Kong Polytechnic University, Hong Kong*
[2]*Monash University, Australia*
(+*Corresponding Author)*
[3]*Security Innovation, Inc., US*
[4]*University of Wollongong, Australia*
[5]*Guangzhou University, China*
[6]*Institute for Infocomm Research, Singapore*
Email: csallen@comp.polyu.edu.hk

Vehicular Ad Hoc Network (VANET) allows vehicles to exchange information about road and traffic conditions through wireless communications. Nevertheless, providing reliable and authenticated information without violating the user's privacy seems contradictory. In this paper, we propose an Anonymous Announcement System especially designed for Electric Vehicle (EV) in VANETs to achieve the aforementioned contradictory goals. We demonstrated the feasibility of the protocol with a prototype implementation on a suitable device and a network simulation with our protocol added on top of a normal VANET.

Keywords: Vehicular Communication, Privacy, Electric Vehicle

1. INTRODUCTION

1.1. VANET

A Vehicular Ad-Hoc Network (VANET) is a technology that allows moving cars as nodes to form an ad-hoc network. In a VANET, every car can be a router or a node. It allows other vehicles to connect and route through data. A network for wide area can be formed. It is *ad-hoc*, in the sense that cars can move out from the single range and drop out of the network, while other cars can join. All connecting vehicles then form a Mobile Ad-Hoc Network (MANET).

VANETs can further provide traffic optimization [31, 35, 46, 12]. Vehicles can serve as data collectors. They can transmit the traffic condition information, such as the number of neighbours and their mean velocities. Within the infrastructure of VANETs, privacy and security are the two major challenges especially if VANET acts as a source of (traffic) information . No driver wants to broadcast his/her real identity and current location while in contrast, authentication is required at the same time. Otherwise, one may send some wrong messages or impersonate others to send messages. There are many schemes in the literature (such as [45, 19, 18, 44]) that deal with these two seeming contradictory requirements.

Chen *et al.* [11] addressed the problem of reliability of information exchange between vehicles. Consider the case in their scenario when a car driver Bob receives a message from another vehicle reporting some traffic jam a few miles away. He may not have any idea whether the message is true or not. At the beginning, he attempts to ignore it. But shortly after that he receives several messages (say n) reporting the same traffic jam. If this number n is a reasonably large number and these messages are sent by n different vehicles, this information is likely to be true, as it seems unlikely that any n vehicles would collude to lie. However, if all these messages are sent anonymously due to privacy concern, how can Bob find out whether n received messages are sent by n different legitimate vehicles without discovering the identities of these vehicles? The scenario is illustrated in Figure 1. The authors proposed a solution using Threshold Anonymous Announcement (TAA) service.

TAA allows every vehicle to obtain a token from a trusted party. One may broadcast an anonymous message to other vehicles signed by this token so that any recipient of this broadcast message may know that it is from a legitimate vehicle yet the identity is unknown. At the same time, TAA provides linkability. That is, if a vehicle sends the same message twice, the

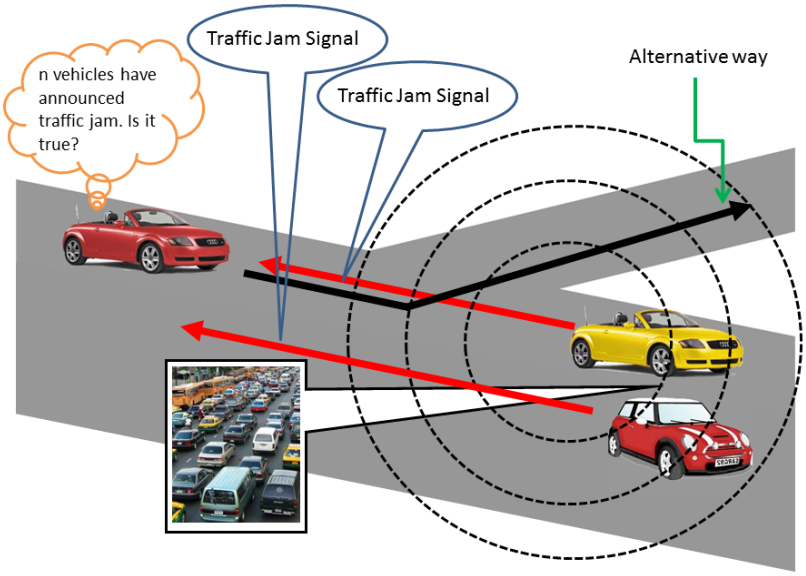

FIGURE 1: Threshold Anonymous Announcement service

receiver will be able to know these two messages are sent by the same vehicle. Hence, it is easy to distinguish whether n messages are from n different vehicles.

Their solution can satisfy some of the security requirements, namely *reliability* (the announcement was issued by a legitimate source without unauthorized modification); *privacy* (a broadcast message cannot be bound to its source and different messages from one source cannot be linked to each other); and *auditability* (if a source is defective or malicious, it can be identified and rejected). However, the verifier in the system cannot ensure that the sender is actually at the claimed position. It uses the simple threshold technique to determine the accuracy. That is, if the number of announcements of the event reaches the predetermined threshold, the verifier believes that the reported event is true and takes appropriate action.

1.2. Electric Vehicle

Electric vehicles (EVs) are propelled by an electric motor (or motors) powered by rechargeable battery packs. Electric motors have several advantages over internal combustion engines (ICEs). Electric motors convert 75% of the chemical energy from the batteries to power the wheels while internal combustion engines (ICEs) only convert 20% of the energy stored in gasoline. Besides, EVs emit no tailpipe pollutants, although the power plant producing the electricity may emit them. Electricity from hydro, solar, or wind-powered plants causes no air pollutants which in turn becomes re-usable energy.

Despite their potential benefits, widespread adoption of EVs faces several hurdles and limitations. One of the major problems is the driving range. Most EVs can only go at most 150 km before recharging, while gasoline vehicles can go at least 500 km before refueling. One of the solutions is to install more fast charging stations with high-speed charging capability so that consumers could recharge the 100 km battery of their electric vehicle to 80 percent in about 30 minutes.

1.3. EV in VANETs: The Advantage

The shortcoming of EV is not really bad. We try to turn it into an *advantage*. Although the frequent charging process may reveal the location information of the EV, on the opposite side, the charging station can *authenticate* the location of the EV. In the scenario described in Section 1.1, the location of each car is not authenticated. The car in location A (pretending it is in location B) may send a message telling others about the traffic condition in location B. Definitely it is not accurate. However, other drivers can do nothing to check the authenticity of the location message. One may use a GPS to provide location information embedded in the message. Nevertheless, without any authentication, the driver may provide a false GPS data instead of the real one. For EV, the charging station provides an excellent way to authenticate the current time and location of the car. The car may get an authenticated token from the charging station, proving that it is within a specific location at a particular time. It then uses this token to sign the current traffic condition and broadcasts to other vehicles. In this way, the accuracy of the whole system can be greatly

improved. Details of the idea will be given in Section 3.2.

1.4. Our Contribution

We propose a solution called Anonymous Announcement System (AAS) for Electric Vehicle in VANETs. Our system can be regarded as the enhanced version of TAA [11]. In addition to the basic features provided in TAA, we also allow an EV to broadcast a message telling nearby vehicles about the current traffic condition. Simultaneously our system protects the privacy of the sender. In general, our system satisfies the following security features:

1. **Entity Authentication with Data Integrity:** If a vehicle accepts a reported event, the announcement was issued by a legitimate source without unauthorized modification.
2. **Location and Time Authentication:** The location of the sender was authenticated by the charging station. That is, the receiver can ensure that the sender was within a particular location at a specific time.
3. **Privacy:** A broadcast message cannot be linked to its source, and different messages from one source authenticated by different charging stations cannot be linked to each other.
4. **Accuracy:** Upon receiving a message, the receiver uses a two dimensional formula to calculate the accuracy of the message: if the authenticated location is farther, the accuracy of this message is lower. Similarly, the longer the authenticated time, the lower the accuracy is. The receiver may receive a number of messages and calculates the overall accuracy based on these two factors.

Furthermore, our system is also compatible with non electric vehicles. Without giving any information about the location and time, a message is regarded as an unauthenticated message and the accuracy is determined as medium. We introduce a special formula to calculate the overall accuracy for a given set of authenticated and unauthenticated messages.

When compared to the TAA, our system not only provides an authenticated way for EV to broadcast traffic condition message, the efficiency is also improved. We allow vehicles (and charging stations) to use idle time to do some pre-computations offline. When it needs to signs a message, it can use the pre-computed data to facilitate the sign process. In addition, different from the TAA, we do not require any pairing operation in our whole system. Pairing is an expensive computation operation which is believed not to be suitable for lightweight and handheld devices. Without pairing operation, our system can be easily implemented in any portable devices or in-car-units.

We would also like to remark that our proposal do not achieve perfectly unlinkability. Roughly speaking, the privacy offered by our scheme is falls between pseudonymity and anonymity. The pseudonym is chosen by the vehicle and cannot be deanonymised to any user identifier. Furthermore, the user refreshes its pseudonym each time it makes a new re-charge. Still, messages sent by the same vehicle using between re-charging are linkable. This is in contrast with TAA, where messages are only linkable for the same event to prevent a malicious node from injecting the messages about the same event into the network multiple times.

2. RELATED WORK

Many schemes have been proposed in the literature to address the issues of authenticity, privacy and accuracy with a variety of mechanisms, with different emphasis and with varying degrees of success. Here we only focus on research that is particularly relevant to these features within a similar framework.

2.1. Crytographyic Solutions

We briefly discuss various cryptographic primitives that could be applied to this specific problem and discuss the obstacles for their directly applications. They are not employed in our system.

2.1.1. Credential System

An anonymous credential or pseudonymous system, first introduced by Chaum [5], is a system in which a user obtains a credential from an issuer and demonstrates the possession of the credential to a verifier who only has the public information of the issuer. Apart from the fact of the user's ownership of a credential granted by an issuer, the verifier cannot get the identity of the user, even if the verifier colludes with the issuer.

There are two types of credential systems: the one-show credential system and the multi-show credential system. Possession of a one-show credential can only be demonstrated once. Otherwise, it can be detected or anonymity of the owner will be compromised. Possession of a multi-show credential can be demonstrated for an arbitrary number of times without being linked and the anonymity of the owner would not be compromised.

Camenisch and Lysyanskaya proposed the first practical multi-show credential system [3]. Their system allows a user to unlinkably demonstrate possession of a credential as many times as necessary without involving the issuer.

These credentials can be used to sign an announcement in VANETS [36, 2, 24, 14, 34, 22, 9] which guarantees authentication and data integrity. However, the issue of distinguishability of origin may arise: are two messages coming from two different sources or one single source? If a single vehicle is able to send multiple messages pretending to come from different sources, then it

would definitely influence the acceptance of announcements.

2.1.2. Ring Signature or Group Signature

Group signatures, introduced by Chaum and Heyst [6] in 1991, allow group members to anonymously sign arbitrary messages on behalf of the group. Verifiers do not know who the actual signer is, but only the fact that the signer is one of the members within the group. In addition, signatures generated from the same signer are unlinkable, that is, it is difficult to determine whether two or more signatures were generated by the same group member. In case of dispute, a group manager will be able to open a signature and incontestably show the identity of the signer. At the same time, no one will be able to falsely accuse any other member of the group. Group signatures may be used in VANETs to provide anonymous authentication purposes [2, 24, 7, 25].

The ring signature concept introduced by Rivest, Shamir, and Tauman [37] improves the privacy preserving capability of group signatures by removing the need for a group manager and allowing a signer to create an ad-hoc group membership even without the knowledge of the other members whose identities and public keys she has used. Ring signature scheme is an excellent primitive for use in applications with the competing requirements of message authenticity and signer privacy. It can also be used in VANETs to provide privacy and authenticity [16, 8].

Nevertheless, similar to credentials, both primitives cannot provide distinguishability of origin. A variant of ring signature may solve this problem. Linkable ring signature was first proposed by Liu *et al.* [27] in 2004. In this notion, the identity of the signer in a ring signature remains anonymous, but two ring signatures can be linked if they are signed by the same signer, no matter whether those two messages are the same or different. Linkability is compulsorily embedded into the signature instead of voluntarily added in linkable ring signatures. If the signer refuses to add the correct linking information, the whole signature becomes invalid. In other words, linkability is enforced by the verifier. The signer cannot decline to do so. This variant provides an option to distinguish two messages of origin: If they are from the same signer, they can be linked.

However, using (linkable) ring signature in VANETs may face another obstacle. How can the user know the identities of nearby vehicles as it is a requirement of ring signature? Assume there are 100 vehicles in a congested area, without the help of any infrastructure, it is impossible to know who is also being congested in this area. That makes ring signature difficult to be deployed in VANET announcement system.

2.2. Anonymous Authentication Schemes for Vehicular Networks

In the area of security and privacy of Vehicular Ad Hoc Networks (VANETs), a number of research works have been done on anonymous authentication to ensure security and privacy. A majority of these schemes make use of pseudonyms (e.g. [2, 45, 18]) or anonymous credentials (e.g. [13, 15]). A recent approach is to use signature-based technique (e.g. [24, 22, 43, 11, 42, 28]) to achieve anonymous authentication. All these schemes are suitable for authorization in different situations with different requirements and features. We pick the one with most similar features with our scheme for detail description.

2.2.1. Threshold Anonymous Announcement (TAA)

Threshold Anonymous Announcement (TAA) was proposed by Chen *et al.* [11]. It uses direct anonymous attestation and one-time anonymous authentication to provide anonymous announcement system. The accuracy was based on a threshold value: If a vehicle receives more than n messages sent by n different vehicles reporting the same traffic jam and if n is reasonably large number, it is likely that the information is true. The TAA system provides a mechanism to ensure that if the receiver accepts the reported event, those n messages are sent by n different vehicles.

Although the accuracy can be determined by the threshold value, there is no way to provide authentication for the location of the sender. The sender may pretend he is in location A while he is actually in location B. There is no mechanism to authenticate the location and time of a vehicle.

2.3. Message Trustworthiness

The trustworthiness of the announcementin a VANET has been studied extensively. Taking location into consideration was studied in [20]. Specifically, Huang et al. concluded that higher trust weighting should be assigned to announcement made by nodes closer to the event. In their work, distance is measured by the number of hops in the network. In another dimension, Li et al. [23] proposed to a reputation-based announcement system in which a central authority maintain and keep track of the reputation of each node so that vehicles could choose to trust messages coming from nodes with a high reputation. Subsequently, Li et al. [29] and Chen et al. [10] further enhances this framework by providing privacy protection to the nodes.

3. OVERVIEW OF THE AAS SOLUTION

3.1. Infrastructure

In our system, there are a system issuer (or authority) and two more entities: charging station and vehicle.

We will not assume the availability of any roadside infrastructure.

The issuer is responsible to certify each charging station. For the charging station, besides the normal charging task, it is also responsible to issue a token for the vehicle, which has embedded the current time and the location information of the charging station. The vehicle uses this token as the signing key, to sign the traffic condition message and broadcasts to other vehicles nearby. After receiving a signed message from other vehicle, the vehicle calculates the accuracy of the message based on the location and time issued for the token. If the location is far away, of course the accuracy should be lower. Similarly, if the issued time is long ago, the accuracy should be also lower.

As the charging frequency for an EV is quite high (e.g. several times a day), the vehicle can get an updated token easily. The message signed by the current token and the message signed by the previous token cannot be linked, even though they are produced by the same signer. This provides unlinkability and privacy to each user. However, the messages produced by the same token can be linked. This is to prevent a single user sending n different messages pretending these messages are sent by n different users. That is, it provides a mean to distinguish the source of origin.

3.2. Basic Idea

The basic idea of our AAS is similar to the TAA system: we all rely on other vehicles to broadcast anonymous traffic condition messages in VANETs. The main difference is that. In the TAA scheme, the vehicle is only authenticated for the *eligibility* to broadcast the message. The accuracy of the message is solely determined by the threshold value. There is nothing related to the location and time. On the other side, our AAS makes use of the property of EV, namely the requirement to re-charge frequently, to provide an authentication mechanism for the location and time of the vehicle. Our system works as follow.

When an EV goes to re-charge, the charging station gives a credential to it. The credential has embedded the current location and time. Later when the EV wants to broadcast a message about the current traffic condition, it first signs the message with this credential and broadcasts the message and signature pair to other vehicles. When a nearby vehicle receives this information, it first verifies the signature and calculates its accuracy based on its authenticated location and time.

We have an index called *accuracy index* which is used to determine the accuracy of the message. We divide it into two parts. For the first part, we set the initial value to be 1. If the authenticated location and the reported location of the incident is near (e.g. within 10km), we multiply the accuracy index by 100%. If the incident location is a bit far away (e.g. between 10km and 20km), we multiply the accuracy index by 80%, and so on. Similar mechanism will be done for the authenticated time and the reported time of the incident. If the time difference between the re-charging and the reported incident is small (e.g. within 10 minutes), we multiply the accuracy index by 100%. If the time difference is larger (e.g. within 10 to 20 minutes), we multiply the index by 80%, and so on.

Besides the location and time difference between the re-charging and the reported incident, we also need to take into account the location and time difference between the reported incident and the receiver. It is used to determine the second part of the accuracy index, which is first initialized to be 1. We use similar formula to calculate it as part one.

Finally we add up the index of part one and part two. The score should be in between 0 and 2. If it is near 0, that means it is not accurate and if it is near 2, that means it is very accurate. This is the accuracy index from *one* vehicle. The concept of accuracy index is illustrated in Figure 2.

We need to add up all accuracy indexes received from other vehicles to determine the final accuracy. If it is above a threshold value, the receiver believes that it is true. This threshold value can be set by the receiver dynamically. Note that our AAS can be also compatible with non electric vehicles. If the received information comes from a normal car (without authenticated location and time), we can set the accuracy index to be 1 (that is, in between very accurate and very inaccurate).

3.3. Adversarial Model

We will adhere to the model in which adversaries constitute a relatively small fraction of the active vehicles at any one time [17, 33]. The aim of an adversary would be to make announcements that would be accepted by other vehicles and thereby mislead them, or to track other vehicles. For example, let us consider a case when a vehicle wants to go from A to B. There are two roads connecting A and B: highway X and highway Y. An adversary may try to announce and convince others that highway X is very congested. As a result, other vehicles may go through highway Y instead. At the end, highway X is empty. The adversary may get advantage of this false announcement.

Another aim of the adversary is to pretend it is in location A at time t_1 while actually it is in location B at time t_2. By providing a false location and time information, other vehicles may be misled by the adversary. It may then gain advantage from it.

3.4. Assumptions

We first assume that a vehicle is equipped with a tamper-resistant black box. We note that this is a common practice in VANET protocol design [33, 22, 11].

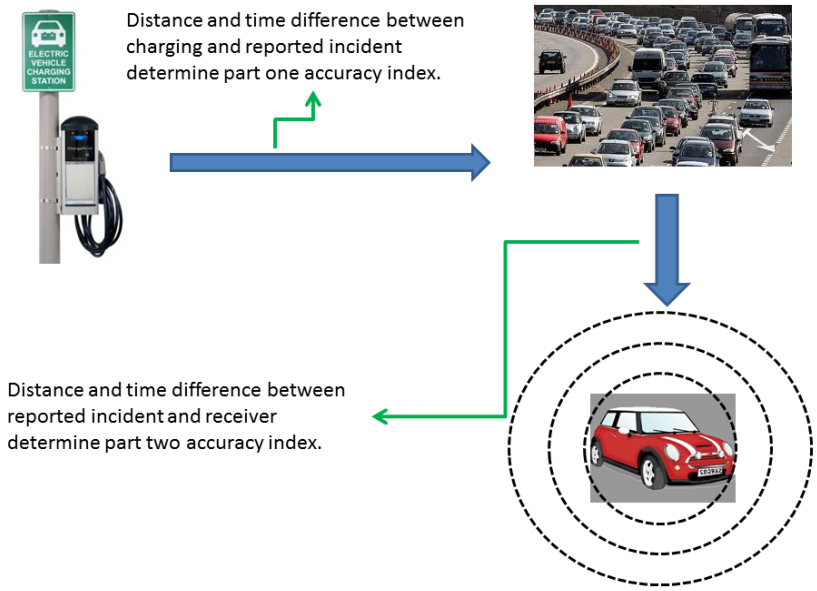

FIGURE 2: The Concept of Accuracy Index

This black box has protection for the secure storage of secrets and a component which can perform basic cryptographic operations securely. We assume it will always operate correctly according to the algorithm, and will never disclose its secrets.

We also assume that there is a system issuer, or an authority, which has its own secret key and the corresponding system parameter is available to all vehicles and charging stations. Each announcement can be verified by using the system parameter.

In addition, we assume that the charging station is trusted. It will only issue a credential to a EV if and only if the EV genuinely recharge for an amount that is higher than a certain threshold. This is to prevent any EV from obtaining multiple credentials through many small-amount recharges.

We further assume that our system is immune to any kind of physical security attack (e.g. any attack within the physical layer, or any physical attack against entities), side-channel attack (that is, any attack based on information gained from the physical implementation of a system, rather than brute force or theoretical weaknesses in the algorithms) or denial-of-service attack. We consider these attacks are out of the scope of this paper.

4. OUR PROPOSED SYSTEM

We now give a detailed description of our proposed AAS system. Our scheme consists of the following protocols: Setup, Certify, Re-Charge, Sign, Verify and Accuracy Calculation.

Setup creates the system secret key which should be stored by some authorities and public parameters. Certify allows each charging station to register with the authority to provide charging service. Re-charge allows users to re-charge their vehicles and get the token used for authenticating their announcement. Sign signs an announcement anonymously using the token obtained from charging station. Verify verifies a signature. Accuracy Calculation calculates the overall accuracy based on the information of different messages received.

4.1. Cryptographic Primitives

We made use of two basic cryptographic primitives, namely, digital signatures and identity-based signatures (IBS) [41]. Indeed, it has been shown in [1] that the former implies the latter and thus it is safe to say our construction is based on well-established primitive from cryptography.

4.2. Concrete Construction

We employ the IBS due to Liu et al.[26] and the standard Schnorr Signature [39] since both of them are efficient and more importantly, support pre-computation.

- Setup: Let k be a security parameter. Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order p such that p is of length k. The authority (e.g. transportation department) selects a random number $x \in_R \mathbb{Z}_p$ and computes $X = g^x$. It chooses a collision-resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$. The public parameters param and the master secret key

msk are given by

$$\mathsf{param} = (\mathbb{G}, g, p, X, H) \qquad msk = x$$

- Certify: Let $\mathsf{ID} \in \{0,1\}^k$ be the identifier of a charging station located at location $\mathsf{Loc} \in \{0,1\}^k$. The authority selects $r \in_R \mathbb{Z}_p^*$ and computes

$$R = g^r \qquad s = r + H(R||\mathsf{ID}||\mathsf{Loc})x \bmod p$$

The secret key of this charging station is (R, s).

- Re-Charge: To speed up things, the protocol is divided into two phases. In the off-line phase, both charging station and the user can perform pre-computation without knowing anything about the re-charge process about to take place. Thus, the idle CPU time can be utilized effectively.
  - Offline Phase. The charging station randomly picks $y \in_R \mathbb{Z}_p^*$ and computes $Y = g^y$. The user randomly picks $u \in_R \mathbb{Z}_p^*$ and computes $U = g^u$.
  - Online Phase. This phase happens when the user re-charge at the charging station at time time. The user sends U to the charging station, who computes $h = H(Y||R||U||\mathsf{time})$[7] and $z = y + hs \bmod p$. The charging station returns (Y, R, z) to the user. User stores the token $(\mathsf{ID}, \mathsf{Loc}, \mathsf{time}, Y, R, z, U, u)$. Note that the user could validate the token by checking

$$g^z = Y(RX^{H(R||\mathsf{ID}||\mathsf{Loc})})^{H(Y||R||U||\mathsf{time})}.$$

- Sign: Again, the user can conduct pre-computation when its CPU is idle.
  - Offline Phase. The user randomly picks $v \in_R \mathbb{Z}_p^*$ and computes $V = g^v$.
  - Online Phase. To create a signature on announcement m, the user with token $(\mathsf{ID}, \mathsf{Loc}, \mathsf{time}, Y, R, z, U, u, V, v)$ computes $c = H(\mathsf{ID}||\mathsf{Loc}||\mathsf{time}||U||V||m)$ and $w = v - cu \bmod p$. Output the signature as

$$\sigma = (\mathsf{ID}, \mathsf{Loc}, \mathsf{time}, Y, R, z, U, c, w)$$

- Verify: To verify a signature σ on announcement m, the verifier first parse σ as $(\mathsf{ID}, \mathsf{Loc}, \mathsf{time}, Y, R, z, U, c, w)$. He/she computes $h = H(Y||R||U||\mathsf{time})$ and $c = H(\mathsf{ID}||\mathsf{Loc}||\mathsf{time}||U||V||m)$. Next, it outputs accept if and only if

$$\begin{aligned} g^z &= YR^hX^{hH(R||\mathsf{ID}||\mathsf{Loc})} \\ c &= H(\mathsf{ID}||\mathsf{Loc}||\mathsf{time}||U||U^cg^w||m) \end{aligned}$$

- Accuracy Calculation:
We use an index, called *Accuracy Index*, to define the accuracy of each message. The index is divided into two parts:

[7] We remark that the time time is specified by the charging station. We do not assume a complete synchronisation of time over the VANET.

TABLE 1: Location Factor

Location Difference	Factor
0 - 10 km	100%
10.01 - 20 km	80%
20.01 - 30 km	60%
30.01 - 40 km	40%
40.01 - 50 km	20%
more than 50 km	0%

TABLE 2: Time Factor

Time Difference	Factor
0 - 10 minutes	100%
10.01 - 20 minutes	80%
20.01 - 30 minutes	60%
30.01 - 40 minutes	40%
40.01 - 50 minutes	20%
more than 50 minutes	0%

1. The first part corresponds to the location and time differences between the previous visited charging station and the reported incident.
2. The second part corresponds to the location and time differences between the reported incident and the receiver.

The initial value of each part is set to be 1. A location factor and a time factor will be multiplied to it, according to the differences of the location and time respectively. The factors can be defined according to different scenarios and environments. Here we just give an example for defining factors, which are presented in table 1 and 2. **We remark that this can be adjusted easily without affecting the technical part. The adjustment can be done according to different situations. We do not cover this part in the scope of this paper.**
After multiplying, the two partial indices will be added up together. Thus the final index will be from 0 to 2. 0 represents the message is very inaccurate, while 2 represents the message is very accurate. For messages sent from non-EV, as there is no authenticated location and time information, we give a medium value for those messages. This "value bar" is shown in Figure 3.

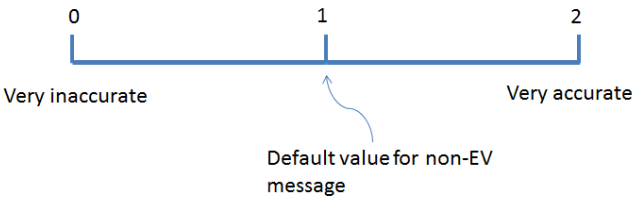

FIGURE 3: Overall accuracy index

We use an example to illustrate how it works.

- After being re-charged at 1pm, a vehicle passed through a location at 1:15pm which is 5 km away from the charging station. There was an accident and traffic jam in that road. At 1:40pm, it arrived at a location which is 13 km away from the accident and it sent a broadcast message telling nearby vehicles about this accident.
  - The first part of the accuracy index is calculated as follow. As the location difference is 5 km (between the charging station and the accident), the location factor should be 100%. As the time difference is 15 minutes, the time factor should be 80%. Thus the first part of the accuracy index should be $1 \times 100\% \times 80\% = 0.8$.
  - The second part of the accuracy index is calculated as follow. As the location difference is 13 km (between the accident and the receiver), the location factor should be 80%. As the time difference is 25 minutes, the time factor should be 60%. Thus the second part of the accuracy index should be $1 \times 80\% \times 60\% = 0.48$.
  - The final accuracy index of this message should be $0.8 + 0.48 = 1.28$.

The above example shows how to calculate the accuracy index for one message. The vehicle also needs to collect a number of messages for the final calculation. Upon received n valid messages, it first discards any repeated messages (sent from the same vehicle) by checking whether any two or more messages containing the same U. Then it adds up the accuracy indexes of all remaining messages. If the final value is above a threshold (e.g. above 10), it decides to believe that the information is true. We also note that these parameter values (e.g. location factor, time factor, overall threshold value) can be adjusted according to different environments. For example, the following formula is used in [20]: a factor of α is given to the first observer of an incident, and the nodes d hops away from the observer is given a factor of α^d. In this paper, we just provide an example showing how to apply our scheme to the actual scenario.

5. SECURITY ANALYSIS

We informally show that our Anonymous Announcement System (AAS) for Electric Vehicle in VANETs provides reliability and privacy. Following our accuracy calculation formula and a threshold of 10, each announcement m endorsed by a signature $(\mathsf{ID}, \mathsf{Loc}, \mathsf{time}, Y, R, z, U, c, w)$ can have an accuracy index of at most 2. To trick a vehicle into believing an announcement, at least five signatures whose value U are distinct are required.

Note that the tuple (Y, R, z) is an identity-based signature on $U||\mathsf{time}$ under the identity $\mathsf{ID}||\mathsf{Loc}$. The tuple (c, w) is a Schnorr signature under the public key U. Due to the unforgeability of both signature schemes, it is impossible for any attacker to create an announcement with a new U value without having recharged at station ID in location Loc at time time. Thus, to trick a vehicle into believing an announcement, collusion of five vehicles is needed.

On one hand, privacy guarantee is straightforward since there is no common identifier for a vehicle across each recharge. Every time the vehicle chooses a new u and compute $U = g^u$, which is unrelated to the value U in the previous re-charge. On the other hand, announcement made by the vehicle using the same U is by default linkable so as to prevent a malicious from posting multiple announcements to affect the decision of others.

6. PERFORMANCE ANALYSIS

6.1. Performance of our scheme

We analyse the performance of our scheme. The implementation was done on a testbed of Lenovo X200s with an Intel Core 2 Duo CPU L9400, 4GB Ram running Windows 7. The software library is MIRACL version 5.2. The code is C and the developing environment is Visual C++ 2008 Express Edition. We use SHA-1 as the hash function [8]. We measured the performance using a 192-bit secret key in elliptic curve cryptosystem (ECC). It is generally believed that a 192-bit secret key in ECC provides stronger security than a 1024-bit key in RSA [38].

The curve we choose is the curve P-192, one of the curves over prime fields recommended by NIST.[9] The curve is defined by

$$\hat{y}^2 = \hat{x}^3 - 3\hat{x} + \hat{b} \bmod \hat{p},$$

where $\hat{b}$ is taken to be 64210519 $e59c80e7$ $0fa7e9ab$ 72243049 $feb8deec$ $c146b9b1$ (in hexadecimal) and $\hat{p}$ = 62771017 35386680 76383578 94232076 66416083 90870039 0324961279 (in decimal). The generator g is at the coordinate (188$da80e$ $b03090f6$ $7cbf20eb$ $43a18800$ $f4ff0afd$ $82ff1012$, 07192$b95$ $ffc8da78$ $631011ed$ $6b24cdd5$ $73f977a1$ $1e794811$) (in hexadecimal) and has an order p = 62771017 35386680 76383578 94231760 59013767 19477318 2842284081.

[8] We remark that in order to enhance the security, SHA-1 can be replaced by a stronger hash function, e.g. SHA-256 or SHA3-256. But for the purpose of this simulation, we simply use SHA-1. Therefore we remark for this security adjustment if the proposed system is deployed in the practical world.

[9] http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

TABLE 3: Performance of the AAS

Process		Running Time (ms)
Setup	Without file I/O	2.658
	Include file I/O	5.6
Certify	Without file I/O	2.904
	Include file I/O	5.152
Re-Charge	Server (Offline)	3.39
	User (Offline)	2.795
	Server (Online)	0.112
	Include file I/O of both user and server	15.4
Sign	User (Offline)	2.735
	User (Online)	0.074
	Include file I/O	4.344
Verify	Without file I/O	10.628
	Include file I/O	12.078

Our implementation is a simple prototype that supports the following five functions. Input and output are read from, and write to, local file directly. The curve parameter is stored in a text file (common.ecs) [10].

- EV setup. Read the curve data from common.ecs into memory, output the public key and private of the authority to public.ecs and private.ecs respectively.
- EV certify ID Loc. Read curve data and key data from common.ecs and private.ecs, output the private key of the charging station of identifier ID at location Loc to the file ID_Loc.key.
- EV re-charge ID Loc. Read curve data and key data from common.ecs and ID_Loc.key, output the token for the user to the file IDLoc.token. The time time is also stored inside the token file. This function conducts both off-line and on-line computation for the user and the charging station. The value U computed at the user side is first stored as a temporary file, and read in by the program again to simulate the process of transmitting U from the user to the charging station.
- EV sign token_name m. Read curve data and token data from common.ecs and token_name.token, output the signature on message m for the user to the file IDLoc.sig. The value of m and time are also stored in the file.
- EV verify sig_file. Read curve data, public key of the authority from common.ecs and public.ecs. Also obtain the m, ID, Loc, time, and the signature from sig_file and output accept or reject.

We summarize our performance in table 3.

We also summarize the output length of each process in table 4. Here we assume the length of ID (the identifier of a charging station), Loc (the location information of a charging station) and time (the current time of the re-charge) to be 100 bytes each.

[10]Source code and executables are available to the editors upon request.

TABLE 4: Length of output

Process	Length (bytes)
Setup (parameter)	72
(master secret key)	24
Certify (charging station storage)	48
Re-Charge (user storage)	420
Sign (signature size)	444

TABLE 5: Comparison of Functionalities

	TAA-1	TAA-2	Our Scheme
Entity Authentication	✓	✓	✓
Location Authentication	×	×	✓
Anonymity	✓	✓	✓
Distinguishability of source of origin	✓	✓	✓
Unlinkability	✓	✓	✓*
Threshold	✓	✓	✓
Revocation	✓	✓	×

We note that if we reduce the length of ID, Loc and time, the length of user storage in Re-Charge and the signature size in Sign can be significantly reduced. Here we use 100 bytes as we provide flexibility for different applications.

6.2. Comparison with other schemes

In this section, we compare our AAS with the most relevant schemes, the TAA schemes [11][11]. Specifically, we conduct our comparison in terms of functionalities and computational cost.

In table 5, we compare the schemes by considering the following functionalities, namely entity authentication [12], location authentication, anonymity, distinguishability of source of origin (whether one vehicle sending multiple messages pretending they are coming from different vehicles), unlinkability (whether a verifier can link a vehicle from two different messages for different events), threshold (the accuracy is determined by a threshold number of vehicles, instead of from one single vehicle) and revocation. We can see that our scheme is similar to the TAA schemes. The main difference is the location authentication which is not provided in their schemes, and revocation is not supported in our scheme. We remark that unlinkability is guaranteed when a node only make one announcement per re-charge.

In table 6, we compare the computational cost. We use E to denote an exponentiation and P to denote a pairing operation. We only compare Sign and Verify as these are the only common processes between these schemes.

Pairing is an expensive computation operation.

[11]In their paper, there are two schemes. We use TAA-1 and TAA-2 to denote.

[12]We remark that EV authentication (the recharging station checks whether an EV is legitimate or not) can be done by other mechanism such as [4]. Readers may refer to [4] for more details.

[hbtp]

TABLE 6: Comparison of Computational Cost

	TAA-1	TAA-2	Our Scheme
Sign	$6E+1P$	$9E+1P$	1E
Verify	$5E+5P$	$8E+5P$	5E

Operation System	Ubuntu 12.04
C compiler	g++ 4.7.2
Simulator	ns2 2.35
Packets Handling	VanetRBC
Moment Handling	RTMM

TABLE 7: software environment of our implementation

According to [40], one pairing evaluation takes at least 7 times slower than an exponentiation. Our scheme does not require any pairing operation. Thus our scheme is very efficient in terms of computational cost, when compared to the TAA schemes.

6.3. Network Simulation

6.3.1. Configuration of the testbed

To evaluate the performance of our scheme when it is deployed on top of a VANET, we implement our scheme using the network simulator *ns2* [30]. We use the *VANET-Skeleton for ns2* (VanetRBC) library [21] for packets transmitting and the *Random Trip Mobility Model* (RTTM) [32] for the vehicular movement. Table 7 gives more details on the software environment of our implementation.

The VanetRBC is an ns2 module to handle packet transmission in VANET. In addition, we defined our own AAS package based on VanetRBC where the major differences between the two are the size of the packets and the cryptographic delay to process the package. Those two data are obtained from our previous implementation of the scheme. Further, to allow some randomness in the simulation, we randomly choose a number between 15 and 20ms which refers to the time a package is signed, compared with 12.078ms in our previous implementation. We assume that the VANET traffic is 1 package per node per second. In comparison, the AAS packet will be broadcast one time only by the nodes close to the incident. We remark that there may be more than one package describing the incident from different source nodes. However, those packages are treated as different VANET packages.

For simplicity, we assume that the transmitting delay is a constant value, and the transmission is always successful with this delay, as long as two nodes are within the transmitting range. Detail setting of the two packages are listed in Table 8.

The movements of the nodes in our implementation follow the random waypoint model as defined in the RTTM [32], which is one of the most popular mobility models. In this model, each node will be assigned with a series of waypoints that are uniformly randomly chosen. The movement of a certain node will follow its waypoints. At each waypoint, the node will randomly chose a velocity to move towards the next waypoint. We remark that this is somewhat a standardized mobility model to evaluate performance of ad-hoc network protocols due to its simplicity and wide availability.

	VanetRBC	AAS package
Transmitting Range	300 meters	300 meters
Transmitting Delay	100 ms	100 ms
Transmitting Interval	300 ms	300 ms
Package Size	250Byte	500Byte
Package Rate	1 per node per second	1 time only
Cryptographic Delay	0	$15 \sim 20$ ms

TABLE 8: Configuration for nodes

6.4. Simulation Settings

The goal of the simulation are two-folded. Firstly, we would like to know the overhead if our system is implemented on top of an existing VANET. Secondly, we would like to know how long it takes for a message to reach all the nodes within the network. We test our scheme in three different scenarios. The first scenario corresponds to a medium sized area ($25X25km^2$) where the nodes are sparsely distributed. The second and third scenarios are for a larger area ($30X30km^2$). The main difference between these two scenarios are the vehicle density. Details of the scenarios are given in Table 9.

We conduct simulations for each scenario on a classic VANET with and without including our system. The steps are described below.

- We firstly simulate a pure VANET, where the network traffic are generated by each node as per configuration.
- Then, to observe the influence of our scheme, at certain time point (i.e., 100 second), we randomly choose a point in the map[13], where all nodes that are close (i.e. within 1 km) to this point will be chosen as the source nodes and broadcast a packet. We remark again that each note will sign on their packets, hence, although all packets are describing a same incident, they are different packets.
- To minimize the influence of randomness, we run the above simulation for 10 times, each time with a new seed for random generator.
- Lastly, we compare the overall traffic of a pure VANET and a VANET incorporating our scheme.

[13]This is achieved by randomly choose x and y coordinator in the map.

	Scenario 1 Medium Area	Scenario 2 Large Area	Scenario 3 Large Area
Size of Area	$25 \times 25\text{km}^2$	$30 \times 30\text{km}^2$	$30 \times 30\text{km}^2$
Number of Nodes	50	125	350
Velocity	$1 \sim 10\text{m/s}$	$1 \sim 20\text{m/s}$	$1 \sim 20\text{m/s}$
Simulation time	500 seconds	500 seconds	500 seconds
Incident time	100 second	100 second	100 second

TABLE 9: Details of the Scenarios

6.4.1. Results

The results are shown in Figures 4, 5 and 6. It can be observed that as the density of the nodes increases, the throughput per each node becomes more stable. From the result of the last scenario, we can see that the average throughput is around 2.7 kbits per second.

Our AAS packets only affect the throughput by no more than 1 kbits per second, when the number of nodes is small. When there are more nodes in the VANET, on average, the affect of AAS packets becomes less important, increasing the average throughput by less than 0.2 kbits per second. It can be concluded that our system does not affect the throughput of the system in a significant manner.

For all the scenarios, it can be observed that the AAS packet cannot be found after 100 seconds of the time following the occurrence of the incident occurs. In other words, the messages reaches all nodes in the network in around 100s.

It is quite nature since the AAS packets are generated one time only, compared with VANET packet. Indeed, it means that all users in this VANET are aware of the incident within 100 seconds using our method.

7. CONCLUSION

In this paper, we presented an Anonymous Announcement System for EV in VANETs. Our scheme allows an EV to make authenticated and anonymous announcement, by making use of the "short driving range" property of EV. We turn this disadvantage into a way to provide authentication of location and time. Accuracy of the received message can be increased. Our scheme is very efficient. Our performance analysis and implementation result show that most operations can be done within a few milliseconds. This is due to the avoidance of the expensive pairing operation.

Future work may include giving rigorous proofs to the security of the proposed system. Another challenge is to explore the possibility to incorporate roadside infrastructure for tracing and revocation purposes.

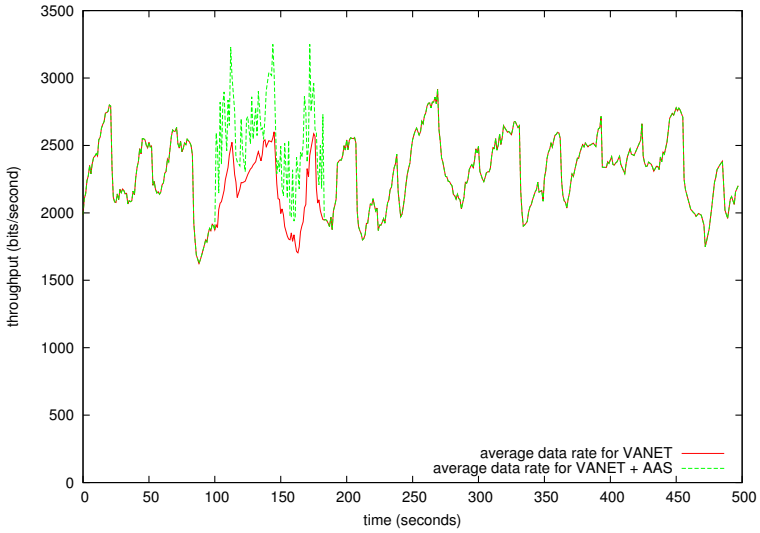

FIGURE 4: Testing Results for Scenario 1

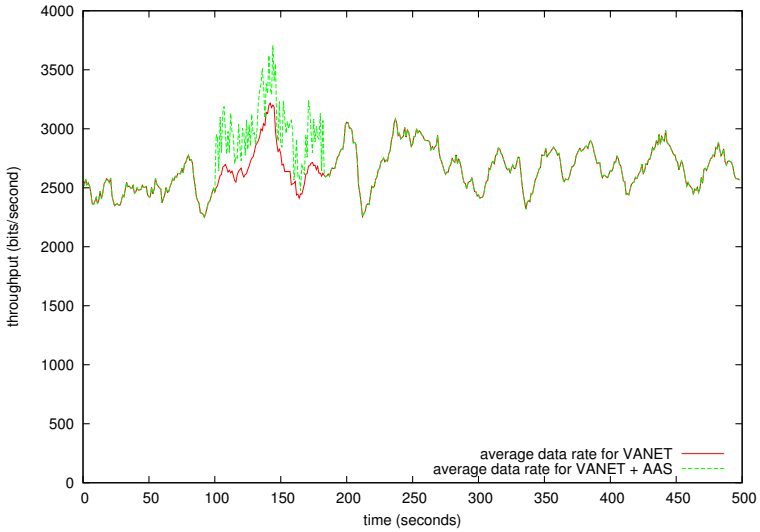

FIGURE 5: Testing Results for Scenario 2

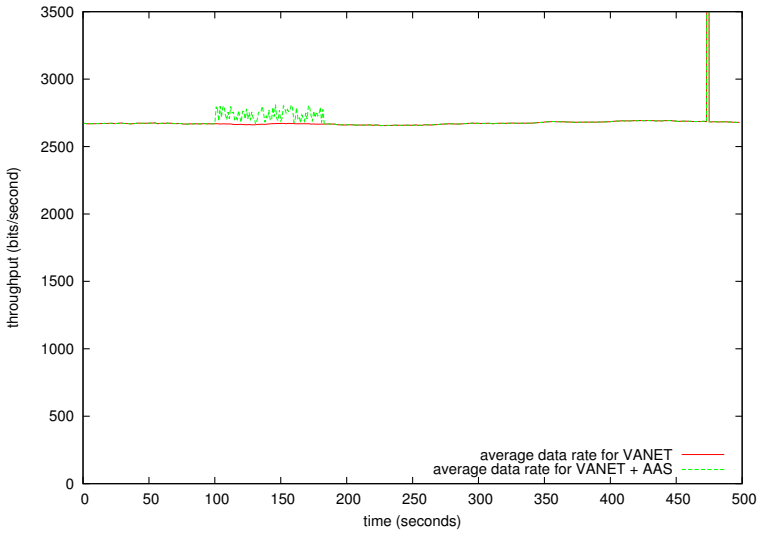

FIGURE 6: Testing Results for Scenario 3

REFERENCES

[1] M. Bellare, C. Namprempre, and G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer, 2004.

[2] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and robust pseudonymous authentication in VANET. In *Vehicular Ad Hoc Networks*, pages 19–28. ACM, 2007.

[3] J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocations. In *EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[4] A. C. Chan and J. Zhou. Cyber-physical device authentication for the smart grid electric vehicle ecosystem. *IEEE Journal on Selected Areas in Communications*, 32(7):1509–1517, 2014.

[5] D. Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, Oct. 2001.

[6] D. Chaum and E. van Heyst. Group Signatures. In *EUROCRYPT 91*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.

[7] B. Chaurasia, S. Verma, and S. Bhasker. Message broadcast in vanets using group signature. In *Wireless Communication and Sensor Networks*, pages 131–136. IEEE, 2008.

[8] B. K. Chaurasia and S. Verma. Conditional privacy through ring signature in vehicular ad-hoc networks. *Transactions on Computational Science*, 13:147–156, 2011.

[9] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar. Pseudonym based mechanism for sustaining privacy in VANETs. In *CICSyN*, pages 420–425. IEEE, 2009.

[10] L. Chen, Q. Li, K. M. Martin, and S. Ng. A privacy-aware reputation-based announcement scheme for vanets. In *5th IEEE International Symposium on Wireless Vehicular Communications, WiVeC 2013, Dresden, Germany, June 2-3, 2013*, pages 1–5. IEEE, 2013.

[11] L. Chen, S.-L. Ng, and G. Wang. Threshold Anonymous Announcement in VANETs. *IEEE Journal on selected areas in communications*, 29(3):605–615, 2011.

[12] W. Cheng, X. Cheng, M. Song, B. Chen, and W. W. Zhao. On the Design and Deployment of RFID Assisted Navigation Systems for VANETs. *IEEE Trans. Parallel Distrib. Syst.*, 23(7):1267–1274, 2012.

[13] T. W. Chim, S.-M. Yiu, L. C. K. Hui, and V. O. K. Li. OPQ: OT-Based Private Querying in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1413–1422, 2011.

[14] V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo. Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. *IEEE Trans. Vehicular Technology*, 58(4):1876–1886, 2008.

[15] A. I. G.-T. Ferreres, A. Alcaide, J. M. de Fuentes, and J. Montero. Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations. *Ad Hoc Networks*, 11(8):2693–2709, 2013.

[16] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum. An identity-based ring signature scheme with enhanced privacy. In *ecurecomm and Workshops*, pages 1–5. IEEE, 2006.

[17] P. Golle, D. H. Greene, and J. Staddon. Detecting and correcting malicious data in vanets. In *Vehicular Ad Hoc Networks*, pages 29–37. ACM, 2004.

[18] D. Huang, S. Misra, M. Verma, and G. Xue. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 12(3):736–746, 2011.

[19] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien. ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks . *IEEE Transactions on Vehicular Technology*, 60(1):248–262, 2011.

[20] Z. Huang, S. Ruj, M. Cavenaghi, M. Stojmenovic, and A. Nayak. A social network approach to trust management in vanets. *Peer-to-Peer Networking and Applications*, 7(3):229–242, 2014.

[21] D. Jungels. VANET-Skeleton for ns2. http://gcorser.weebly.com/install-vanetrbc.html, 2005.

[22] G. Kounga, T. Walter, and S. Lachmund. Proving reliability of anonymous information in VANETs. *IEEE Trans. Vehicular Technology*, 58(6):2977–2989, 2009.

[23] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang. A reputation-based announcement scheme for vanets. *IEEE T. Vehicular Technology*, 61(9):4095–4108, 2012.

[24] X. Lin, X. Sun, P.-H. Ho, and X. Shen. GSIS: Secure vehicular communications with privacy preserving. *IEEE Trans. Vehicular Technology*, 56(6):3442–3456, 2007.

[25] H. Liu, H. Li, and Z. Ma. Efficient and secure authentication protocol for VANET. In *CIS*, pages 523–527. IEEE, 2010.

[26] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. Wong. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security*, 9:287–296, 2010.

[27] J. K. Liu, V. K. Wei, and D. S. Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In *ACISP 2004*, volume 3108 of *Lecture Notes in Computer Science*, pages 325–335. Springer, 2004.

[28] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo. Improvements on an authentication scheme for vehicular sensor networks. *Expert Syst. Appl.*, 41(5):2559–2564, 2014.

[29] A. Malip, S. Ng, and Q. Li. A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks. *Security and Communication Networks*, 7(3):588–601, 2014.

[30] S. Mccanne, S. Floyd, and K. Fall. ns2 (network simulator 2). http://www-nrg.ee.lbl.gov/ns/.

[31] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea. VANET Routing on City Roads Using Real-Time

Vehicular Traffic Information. *IEEE Trans. Vehicular Technology*, 58(7):3609–3626, 2009.

[32] S. Palchaudhuri, J. Y. Le Boudec, and M. Vojnovic. Perfect Simulations for Random Trip Mobility Models. In *Proc. of the 38th annual Symposium on Simulation*, number 72–79, 2005.

[33] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications magazine*, pages 100–109, November 2008.

[34] P. Papadimitratos and J.-P. Hubaux. Report on the "secure vehicular communications: results and challenges ahead" workshop. *Mobile Computing and Communications Review*, 12(2):53–64, 2008.

[35] D. B. Rawat, D. C. Popescu, G. Yan, and S. Olariu. Enhancing VANET Performance by Joint Adaptation of Transmission Power and Contention Window Size. *IEEE Trans. Parallel Distrib. Syst.*, 22(9):1528–1535, 2011.

[36] M. Raya, A. Aziz, and J.-P. Hubaux. Efficient secure aggregation in vanets. In *Vehicular Ad Hoc Networks*, pages 67–75. ACM, 2006.

[37] R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

[38] M. Robshaw and Y. Yin. Elliptic curve cryptosystems. An RSA Laboratories Technical Note, 1997.

[39] C.-P. Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3):161–174, 1991.

[40] M. Scott. Efficient implementation of cryptographic pairings. http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf, 2007.

[41] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[42] K.-A. Shim. Cpas: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. *IEEE T. Vehicular Technology*, 61(4):1874–1883, 2012.

[43] J. Sun, C. Zhang, Y. Zhang, and Y. Fang. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.*, 21(9):1227–1239, 2010.

[44] Y. Sun, Z. Feng, Q. Hu, and J. Su. An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. *Security and Communication Networks*, 5(1):79–86, 2012.

[45] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE T. Vehicular Technology*, 59(7):3589–3603, 2010.

[46] B. Yu, C.-Z. Xu, and M. Guo. Adaptive Forwarding Delay Control for VANET Data Aggregation. *IEEE Trans. Parallel Distrib. Syst.*, 23(1):11–18, 2012.