Xi Y, Sha KW, Shi WS *et al.* Probabilistic adaptive anonymous authentication in vehicular networks. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 23(6): 916–928 Nov. 2008

Probabilistic Adaptive Anonymous Authentication in Vehicular Networks

Yong Xi[1] (习　勇), Ke-Wei Sha[1] (沙科伟), Wei-Song Shi[1] (施巍松), Loren Schwiebert[1], and Tao Zhang[2] (张　涛)

[1] *Department of Computer Science, Wayne State University, Detroit, Michigan, U.S.A.*

[2] *Telcordia Technologies, Inc., New Jersey, U.S.A.*

E-mail: {yongxi, kewei, weisong, loren}@wayne.edu; tao@research.telcordia.com

Received October 24, 2007; revised September 16, 2008.

Abstract Vehicular networks have attracted extensive attention in recent years for their promises in improving safety and enabling other value-added services. Most previous work focuses on designing the media access and physical layer protocols. Privacy issues in vehicular systems have not been well addressed. We argue that privacy is a *user-specific* concept, and a good privacy protection mechanism should allow users to select the levels of privacy they wish to have. To address this requirement, we propose an adaptive anonymous authentication mechanism that can trade off the anonymity level with computational and communication overheads (resource usage). This mechanism, to our knowledge, is the first effort on adaptive anonymous authentication. The resources used by our protocol are few. A high traffic volume of 2000 vehicles per hour consumes about 60kbps bandwidth, which is less than one percent of the bandwidth of DSRC (Dedicated Short Range Communications). By using adaptive anonymity, the protocol response time can further be improved 2∼4 times with less than 20% bandwidth overheads.

Keywords anonymous authentication, vehicular network, privacy, adaptive anonymity

1 Introduction

About half of the 43 000 deaths that occur each year on U.S. highways result from vehicles leaving the road or traveling unsafely through intersections. Traffic delays waste more than a 40-hour workweek for peak-time travelers[1]. Fortunately, with the development of micro-electronic technologies and wireless communications, it is possible to install an On-Board-Unit (OBU), which integrates the technologies of wireless communications, micro-sensors, embedded systems, and Global Positioning System (GPS), on vehicles. With these devices, vehicles can communicate with each other or with roadside units (RSU) connected to Internet. Thus, vehicles, RSUs and the backbone networks form a vehicle infrastructure integration (VII) system[1]. VII collects traffic and road information from vehicles, and delivers road services including road warning and traffic information to users in the vehicles. Thus, a great deal of attention has been put into designing and implementing similar systems in the past several years[2,3].

Current research in VII mainly focuses on vehicular communications. Significant progresses have been made in media access (MAC) layer protocols[4] and physical layer protocols[5]. However, issues about security and privacy, which will play a critical role in the acceptance of the VII system, have not been well studied. Vehicles and the networks need to authenticate each other. Several previous efforts[6−15] have been made to protect user privacy in the authentication process, but most of them use a policy that places trust on the RSUs or the authentication servers in the network. That is, these trusted RSUs or authentication servers can track the locations and activities of vehicles and their drivers. Concerns about security and privacy may prevent vehicle owners from joining this system. We argue that we need to provide vehicle owners with better privacy through anonymity, i.e., no one can trace their activities based on the information provided for the authentication purpose. In this paper, we analyze security and privacy requirements and challenges with the assumption that there is zero-trust of authentication servers. Among these requirements and challenges, we observe that privacy is treated as a one-size-fits-all concept in previous research efforts. However, we argue that privacy is a *user-specific* concept in the sense that different users may have varying privacy requirements. Moreover, a higher privacy requirement usually results

Regular Paper

in more computational or communication overheads. A trade-off should be made between the privacy level and resource usage to meet overall system design goals such as scalability and real-time response. Thus, we propose an adaptive group-based anonymous authentication protocol that is able to trade off the level of anonymity with resource usage. Both analytic results and preliminary simulation results show that the protocol provides promising performance in a real system. In summary, the main contributions of this paper are: 1) we analyze the system design requirements from the view of security and privacy and define the challenges to achieve these requirements; 2) we propose and evaluate an adaptive anonymous authentication protocol; 3) we introduce the concept of adaptive anonymity and discuss the trade-off between the level of anonymity and resource usage.

The rest of the paper is organized as follows. We analyze the requirements and challenges of security and privacy design in VII in Section 2. The application scenario of the authentication protocol in a VII is described in Section 3. In Section 4, a privacy-preserving authentication protocol for the zero-trust model is proposed, and the performance evaluation of the proposed protocol is done in Section 5. Finally, related work is discussed in Section 6 and conclusion is drawn in Section 7.

2 Requirements and Challenges

VII can improve driving safety. However, due to the extremely large system scale, the fast movement of vehicles, and the broadcast nature of wireless communications, there are several requirements and challenges in designing and deploying such a system. The challenges related to security and privacy include the following.

• *Adaptive Anonymity*: mobile users may be concerned with two types of privacies: location and identity privacy (when users/vehicles communicate with the network or with each other) and the privacy about the service usage pattern (when a user/vehicle requests services from service providers). Furthermore, privacy is a *user-specific* concept; some users are more serious about their privacy than others. Thus, we argue that the VII should support multiple anonymity levels, and each user should be allowed to choose his own anonymity level. The authentication protocol should support the trade-off between the anonymity level and resource utilization according to the user's specific privacy requirements.

• *Scalability*: VII is designed for nation-wide applications which may involve millions of vehicles and a large number of service providers. As a result, scalability is a key challenge for the design of this system. During traffic congestion, a large number of authentication requests may overload a local authentication server. The problem of how to avoid the clogging caused by the burst of the authentication messages should be analyzed and tackled.

• *Real-Time Response*: VII is designed to collect road condition data as well as provide mobile services to moving vehicles. Both information collection and service delivery have real-time requirements, especially when a vehicle needs immediate help. Because authentication needs to be performed before data can be collected and the service can be delivered, the authentication process has a strict real-time requirement. Furthermore, the fast movement of the vehicles and the short radio coverage range of the roadside units also require authentication to be finished in a very short time. This suggests that the authentication protocols should be light-weight.

• *Data Security*: collected data should be consistent with raw data on the road. Faked data should be filtered and data modification during transmission should also be prevented. The broadcast nature of wireless communications makes eavesdropping easier, thus, technologies are needed to prevent this kind of attacks. In addition, only authenticated OBUs can use the provided services and OBUs should only access services provided by legitimate service providers. It will be a challenge to detect faked data and locate an attack, especially in the case of anonymous authentication and data reporting.

• *High Availability*: customers of this system may request authentication at anytime and anywhere when they are on the road. Availability is a critical design issue and an important metrics to evaluate the quality of the VII. Secure protocols are essential to preventing the attacks that interrupt these services, especially distributed denial of service (DDoS) attacks. Moreover, load balancing algorithms from traditional distributed system research should be applied to balance the load and relief the clogging.

• *Service Differentiation*: various services will be provided by both private service providers (e.g., automakers and other private companies offering services to the vehicles) and public service providers (e.g., government agencies). Those services need to be differentiated based on the priorities of services and the prices that customers have paid. However, there is a dilemma between service customization and user anonymity. On one hand, a good resource allocation algorithm should provide customized services for each individual. On

the other hand, differentiating services based on specific customer requirements will violate the anonymity requirement of the system.

In this paper, we intend to address the first three requirements in an authentication protocol, i.e., adaptive anonymity, scalability, and timeliness. Other issues will be the objectives of our future work.

3 Problem Statement

In this paper, we address privacy preserving authentications in vehicular networks. Specifically, we intend to protect identity privacy in authentications. We first describe the motivation in applying group-based anonymous authentication to protect identity privacy in Subsection 3.1. We then discuss how to provide adaptive anonymity in this context in Subsection 3.2.

3.1 Anonymous Authentication

Authentication is normally based on the proof of certain knowledge that is established earlier. A typical authentication scenario in vehicular networks is depicted in Fig.1. To prevent overload to a central authentication server and improve its responsiveness that is typically required in vehicular networks, the authentication is delegated to RSUs. The enabling cryptographic technique is public key cryptography, that is, given its public key, anyone is able to verify an OBU's knowledge of the corresponding private key by using public key cryptography. Although all components in Fig.1 can communicate with each other, in this paper, we focus on the authentication process between the vehicles and the RSUs.

VII may support two types of servers: the public servers controlled by government agencies such as the federal or local Departments of Transportation (DoT)

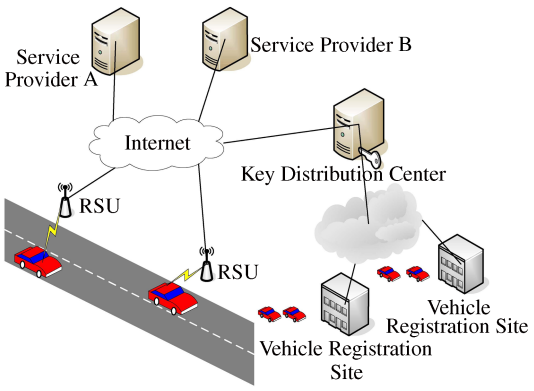


Fig.1. Typical authentication scenario.

and the private servers controlled by the private service providers. Mobile users may want to use different trust policies depending on whether they are communicating with a public or private server (or application). These trust policies include 1) *the full-trust* in which the users trust both types of servers, 2) *the partial-trust* in which the users trust the private or public only, and 3) *the zero-trust* in which the users trust neither of these two types of servers. Most previous researches, such as [6, 16], take the partial-trust policy that trusts some public servers. With these approaches, the authentication requests are sent to some anonymity sever first. Then, the anonymity server sends the anonymized or aggregated requests to other service servers. Thus, anonymity is achieved at the anonymity server level. However, we argue that higher level anonymity is needed from the perspective of mobile users, who do not want the network operators or others to track their daily activities. In the partial-trust model, the trusted servers have the authentication information, e.g., identity of the mobile user, which can be used to easily track the activities of each individual mobile user based on the spatial-temporal analysis such as MTT algorithm[17]. In this paper, we focus on the zero-trust model, i.e., the users will trust no server in the network.

In order to preserve privacy without any server support, we use group-based anonymous authentication. That is, an OBU only proves its membership within a group of OBUs, avoiding exposure of its exact identity.

3.2 Adaptive Anonymity

The anonymity through group-based anonymous authentication is essentially a k-anonymity concept. The tunable parameter k is one aspect of adaptivity for adaptive anonymity. In this paper, we introduce confidence as an extra dimension in the adaptivity of the k-anonymity to reflect personal preference. For example, a user may accept an anonymity level of 30 with a probability of 0.9 guarantee. The use of this probabilistic anonymity does not compromise user privacy. For example, an anonymity level of 30 implies 3.33% chance of being identified. The probability of 0.9 guarantee merely slightly increases the chance of being identified. To guarantee privacy, the confidence as a personal preference should also be hidden from the network.

Another way to implement unconditional k-anonymity is to use ring signature[18]. However, the generation and verification of a ring signature are linear to k. The achieved anonymity is transparent to both sides of the communication. Thus it does not protect the personal preference.

In the next section, we describe the mechanisms of

the probabilistic anonymity and show its advantages in detail.

4 Privacy-Preserving Authentication

Our anonymous authentication protocol is based on a cryptographic construct called *verifiable common secret encoding*[19]. Using *verifiable common secret encoding* enables us to provide adaptive anonymity.

4.1 Verifiable Common Secret Encoding

The *verifiable common secret encoding* is based on public key cryptography. For a group of n users, each with its public/private key pairs (Pub_i, Pri_i), the verifiable common secret encoding is constructed as $(Pub_1(x), Pub_2(x), Pub_3(x), \ldots, Pub_n(x))$. Any member i of the group can decrypt its corresponding encoded message $Pub_i(x)$ with its private key Pri_i, obtaining x'. It encrypts x' with the other $n-1$ public keys to obtain its own copy of the encrypted secrets $Pub_1(x'), Pub_2(x'), \ldots, Pub_n(x')$. It then verifies that these secrets match those that were received. If they all match up, it accepts the secret value x' as x and proceeds with remaining protocol steps.

4.2 Key Management and Group Formation

Each vehicle possesses a pair of public/private keys. Then vehicles are grouped together. The group is initialized and managed in the way described below.

A central server manages group information. For each group member, we build a pair of public/private keys, assign an index to that key pair, and maintain a group version. These members are kept as dummy members before they are assigned to new vehicles, which is usually done by the second level key distribution servers. If the key distribution server and the central server are not cooperating, although there are a lot of dummy keys in each group, the central server has no idea about which key is already issued. If they cooperate, we can delay the function of the whole system until all groups have enough keys distributed. After initialization, all the keys in the group are organized to a complete binary tree, whose breadth-first travel results in an ordered sequence of the corresponding key index. Each subtree root is assigned an ID, which will be used by any member of the subtree in the authentication process. Each vehicle stores IDs of all the subtrees it belongs to.

The dynamic group management is conducted in the following ways. When the keys are revoked, the previous member who holds the key is no longer valid. Thus, the central server will replace the invalid key with a new key pair and update the group version. When a new member joins in, assuming the central server has the information about the number of dummy keys in each group, it will be put into a group with most dummy keys, and the server will find the first dummy or empty slot in the key tree based on a breadth-first search and distribute the corresponding private key, the key index, the group version, and the public key of the whole group, to the new joined member. The updated group information should be distributed to the authentication server and other members in the group, which is a challenge in a large distributed system such as vehicular networks. Fortunately, we can assume that the membership updating is not so frequent. For example, assume that a vehicle will be removed from a group if it is stolen. In US, the average number of vehicles stolen in 2003 is 1 in 190[20]. For a group with 100 vehicles, there is about 50% chance that one vehicle in the group is stolen per year. This is a very small change for the group. When a group is changed, a push approach is used to update the group information to the caching servers. The updating of group information to the group member is integrated with the process of the authentication.

4.3 Protocol Description

The protocol is depicted in Fig.2. It has 4 steps.

1) RSU→OBU: $Cert(Pub_s)$.

RSU announces its presence periodically with its certificate.

2) OBU→RSU: $Pub_s(GID, T_1, V_G, K_{\text{session}}, \textit{ID-Tree})$.

OBU constructs a message with its group identifier *GID*, current time T_1, its current group version V_G, a session key K_{session} selected by itself, and a subgroup identifier *ID-Tree*. It then encrypts the message with RSU's public key Pub_s so that only the RSU is able to decrypt it.

3) RSU→OBU: $K_{\text{session}}(GPub_{\textit{ID-Tree}}(x), T_2, V_G, Pri_s(H))$.

RSU constructs the verifiable common secret for the subgroup *ID-Tree* of the group *GID* with a random value x. It then constructs the challenge message with the verifiable common secret, its current time T_2, its current group version V_G, and the signature $Pri_s(H)$ obtained through encrypting the message hash H with its private key Pri_s.

4) OBU→OBU: $K_{\text{session}}(x, Req, T_3)$.

OBU decrypts x from the verifiable common secret and verifies anonymity guarantee. Upon successful decryption and verification, it constructs a reply message

with x, service request *Req*, and its current time T_3. The message is encrypted with the session key K_{session}.

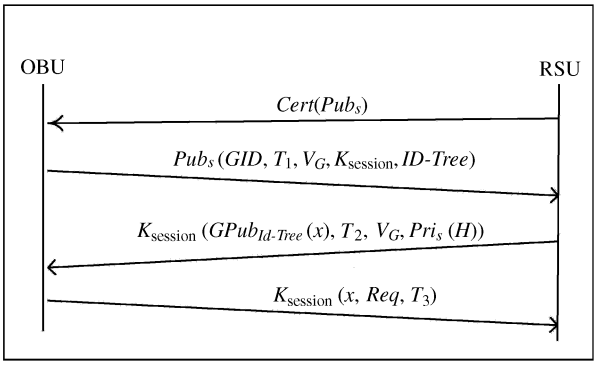


Fig.2. Group-based authentication protocol.

4.4 Adaptive Anonymity

Our protocol provides dynamically adaptive anonymity. Notice that the maximal level of anonymity is bounded by the group size. The adaptive anonymity achieves anonymity levels below this maximal anonymity.

The adaptive anonymity is achieved through tuning two dominating factors within the protocol: communication cost and computation cost. The communication cost is tuned by changing the *ID-Tree* used in the protocol. By changing it to a different one at a different level of the group tree, the subgroup size changes and the size of the challenge message changes. The computation cost is tuned by using probabilistic verification at OBUs. In probabilistic verification, instead of computing all the $n-1$ encrypted secrets $Pub_1(x'), Pub_2(x'), \ldots, Pub_n(x')$, OBU computes m $(m < n-1)$ encrypted secrets randomly chosen out of the $n-1$ secrets and compares only these secrets with the m corresponding secrets that were received. Because the computation cost of public key encryption is relatively expensive, by changing m, the computation cost is changed.

4.5 Analysis of Probabilistic Verification

The probabilistic verification is illustrated with the following example. If the common secret set includes 50 encrypted values, and each encrypted value has a probability of 60% to be verified, as a result, about 30 encrypted values are verified on average, and a lot of computation cost is saved. However, probabilistic verification introduces a risk of the OBU suffering from a reduced level of anonymity. The RSU might use different random values to construct the 50 encrypted values. It then identifies the OBU based on the value returned from the OBU. We call the use of different random values server probing. Next we analyze the effect of the probabilistic verification on the anonymity in the cases of both with and without server probing.

Without server probing, probabilistic verification will not affect the anonymity because the same value is encrypted in all common secrets. We analyze the anonymity in this case. In our protocol, the OBU may choose different sub-trees in each authentication. Thus, it is impossible for the RSU to link these trees to figure out the identity of the OBU by using the spatial-temporal analysis. The RSU has to guess the ID of the OBU by chance. Then, the anonymity that can be expected is determined by the number of nodes in the tree, denoted as $|T|$ and bounded by the depth of the tree, d, where $2^d \leqslant |T| \leqslant 2^{d+1}$. The probability of successfully guessing the vehicle's identity is the multiplicative inverse of the number of nodes in the sub-tree. For instance, in the extreme case of only one member in the sub-tree, the RSU can easily know the person that is communicating with him. For a sub-tree with $|T|$ nodes, the RSU has only a $1/|T|$ probability to identify who is talking with him even when the authenticator knows which vehicles are in this group. The maximum anonymity can be expected in the case that the RSU is not actively probing the identity of the OBU.

In the case of the RSU trying to probe the OBU's identity, the anonymity of the OBU may be reduced. If the RSU wants to identify the OBU exactly, it has to use different numbers for different members. In such a case, the OBU can easily detect the probing by verifying only one other slot. So, let us assume that the RSU is just trying to decrease the anonymity level of the OBU by using the same number for a subgroup of s slots, which is not distinguishable to the RSU. In this case, if the OBU verifies only m slots where $m < s$, the probing may not be detected by the OBU. However, we will show that the probability of the probing not being detected, Pr, is very small.

Assume that there are $|T|$ members in the sub-tree. Then, the probability of probing not being detected is (please see Appendix for derivation)

$$\begin{aligned} Pr &= \frac{C_{s-1}^{m}}{C_{|T|-1}^{m}} \\ &= \frac{(s-1)(s-2)\cdots(s-m)}{(|T|-1)(|T|-2)\cdots(|T|-m)}. \end{aligned}$$

We define the *anonymity reduction factor* r as the ratio of the size of the subgroup to the size of the original

group:

$$r = \frac{s}{|T|}.$$

We have:

$$\frac{s-i}{|T|-i} < \frac{s}{|T|} \quad \text{for} \quad i > 0.$$

So,

$$Pr < \Big(\frac{s}{|T|}\Big)^m = r^m.$$

This means that the probability of successful probing by the RSU decreases exponentially as the number of verifications done by the OBU increases. The rate of decrease is proportional to the anonymity reduction factor. So the RSU cannot reduce the anonymity significantly. Otherwise, the probing by the RSU is easily detected. For example, let $m = 20$, $Pr = 0.01$, then r must be greater than 0.79. In this case, if $|T|$ is 100, then the OBU can be confident that it can detect the reduction of the anonymity up to 79 with probability 0.99 even if only 20 slots are verified. Fig.3 shows the relationship between the anonymity reduction factor and the probability of the reduction being detected with fixed value of $|T|$ and m.

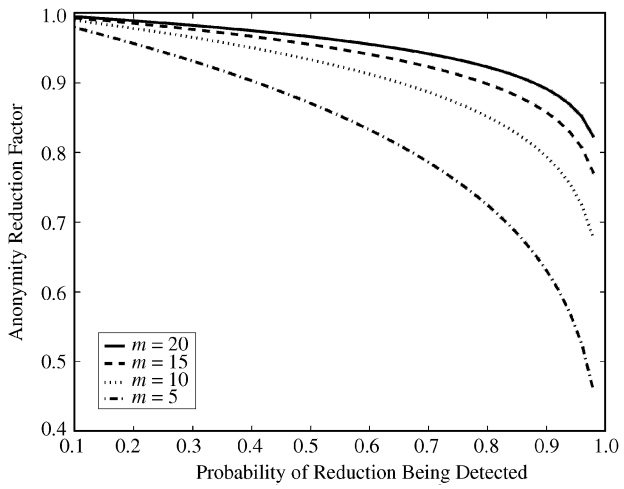


Fig.3. Relationship between probability of detecting reduction and anonymity reduction factor.

The above analysis shows that if we use a probabilistic anonymity definition, it is more flexible in choosing the protocol parameters. So we define the privacy as a tuple, $\langle P, A\rangle$, where A is the anonymity level and P is probability that the achieved anonymity is greater than A. We have shown that there is a mapping between the expected anonymity, which is $\langle P, A\rangle$, and the two parameters in the protocol, the number of the nodes in the tree, $|T|$, and the number of verifications done by the OBU, m. Thus, based on these two parameters we can estimate how much privacy can be expected by the mobile user. Based on the expected privacy requirements, the mobile user can set up the correlation between the two parameters.

To measure the confidence P of anonymity level, given a successful verification by an OBU, we need to calculate the conditional probability of the anonymity level beyond a certain anonymity level A. Since RSU cannot predict which slot the OBU will verify, we can assume that RSU picks each slot uniformly. Assume that RSU assigns the same challenge value used for the OBU to a slot with probability $s/|T|$. We model the problem as a coin tossing problem, in which head represents assigning the same challenge value, tail otherwise. For a coin tossing problem with $r = s/|T|$ as the probability of obtaining heads in a single toss of the coin, the posterior probability r conditional on the number of heads H and the number of tails T is the following:

$$f(r|H = h, T = t) = \frac{(h+t+1)!}{h!t!} r^h (1-r)^t.$$

Denote the event that the verification is successful as V. V corresponds to the event $h = m \cap t = 0$. Substituting r with $s/|T|$, we obtain:

$$f\Big(\frac{s}{|T|}|V\Big) = (m+1)\Big(\frac{s}{|T|}\Big)^m.$$

The confidence that the anonymity level is beyond A is:

$$\begin{aligned} P &= Pr(A < s \leqslant |T||V) \\ &= \int_A^n (m+1)\Big(\frac{s}{|T|}\Big)^m \mathrm{d}\Big(\frac{s}{|T|}\Big) \\ &= 1 - \Big(\frac{A}{|T|}\Big)^{m+1}. \end{aligned}$$

Given specific values of m and $|T|$, high anonymity level can be achieved with low confidence and low anonymity level can be achieved with high confidence.

If we have determined the values of P and A, we can find the relationship between $|T|$ and m,

$$\Big(\frac{A}{|T|}\Big)^{m+1} < 1 - P. \tag{1}$$

To achieve a given anonymity level A and its confidence P, the OBU can either choose a large $|T|$ or a large m. The relationship is shown in Fig.4.

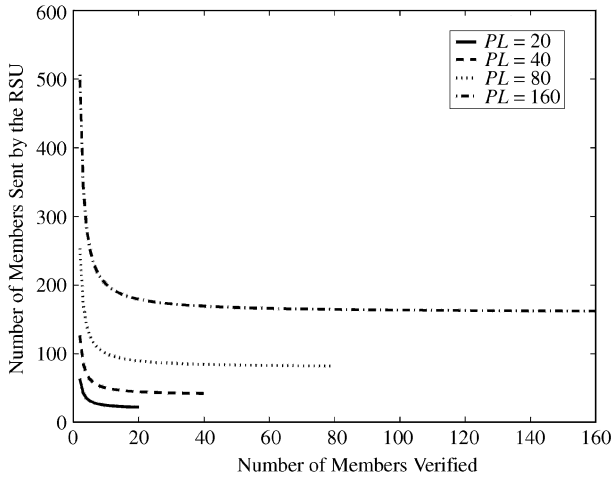


Fig.4. Relationship between the number of members verified and the number of members sent. We use $P = 0.9$ for all cases.

In Fig.4, the x-axis is the number of members being verified while the y-axis is the corresponding total members that should be requested from the RSU. The figure shows that when the OBU verifies only 20 members, the number of members being sent approaches the minimum required values in all the four cases. It also shows that the increased number of members being sent is exponential to the decreased number of members being verified for small values of m. So it is generally preferable to use a reasonably large m. It also shows the effectiveness of the probabilistic verification and discourages the RSU from reducing the anonymity level since the reduction can easily be detected by the vehicle with much lower cost.

The above analysis assumes that the vehicle requires a certain anonymity level and investigates the trade-off between anonymity level and the communication and computational costs. It is our conjecture that, for the purpose of reducing both communication cost and computational cost, the anonymity level has to be reduced. The reduced anonymity level can be specified with a reduced P, a reduced A, or both.

4.6 Intrusion Isolation and Key Revocation

Intrusion detection is necessary to identify an attack. When an attack is detected, we could leverage several communication techniques such as DSRC[5] and GPS to locate the attacker based on the communication between the attacker and the server. When the attacker is located, several follow-up actions can be taken. For example, a message can be sent to a pre-installed device in the vehicle to forbid its wireless communication; under proper situations, a message can be sent to the attack source to disable the vehicle; or a policeman can be sent to that location to catch the attacker[21].

It is not sufficient to only isolate the attack because the attacker may try to authenticate himself using the same key at a different location or on another vehicle. Thus, key revocation is necessary. In our design, key revocation is integrated seamlessly with the group management and the process of authentication. When an attacker is reported, the public key of the attacker will be removed from the group. When the attacker uses the revoked key, the RSU will send it the challenges encrypted by the valid public keys in the group. Since the attacker's public key has already been removed from that set, the attacker will not be able to decrypt the challenge. In this way, the key is automatically revoked and the other members in the group will not be affected.

4.7 Possible Attacks and Defenses

We describe several possible attacks and their defenses below.

Group Reduction Attack. Since our protocol is adaptive, malicious parties may trick OBU into using a lower level of anonymity. We categorize this attack into two classes, *outside attack* and *inside attack*. In the outside attack, a malicious outsider may temporarily overload the network and force an OBU to use a lower level of anonymity. In the inside attack, an RSU may delay the update of group information. The OBU will be using a polluted group under this attack.

The outside attack is a type of denial-of-service (DOS) attack. As far as the authors know, there is no efficient defense against DOS attack in vehicular networks. Instead, we rely on the OBU's policy. In case that anonymity level is dropped below a certain level, the OBU will give up accessing the network.

The following defense against the inside attack is used. The group version V_G is generated in the following way. The KDC periodically generates the hash code of a group. The hash code is then signed by the KDC, along with its update time. The RSU is required to attach V_G along with its challenge. Upon detecting that the code is too old, the OBU will stop interacting with the RSU.

Link Attack. During traveling, an OBU may use different levels of anonymity at different RSUs. If those different requests can be linked to the same OBU, an OBU can only enjoy the smallest anonymity level among those requests. To improve the unlinkability in our protocol, a set of pairs of keys are stored in each OBU. Each key pair belongs to a different group. An OBU rotates its use of the keys.

Compromised OBU. A compromised OBU has no effect on other members of the group. It can access only

the public keys of the other members, which can be released publicly. Due to that the session key from one OBU can be decrypted by the RSU, a compromised OBU is not able to eavesdrop on the conversation between another group member and the RSU.

5 Performance Evaluation

We built a simulator to evaluate the performance of the proposed scheme in a wireless environment. The simulator is based on GlomoSim[22]. We modified GlomoSim to incorporate computation delays introduced by the authentication protocol. The computation delays are obtained by measuring them with sample implementations in OpenSSL. We measured the public key encryption delays associated with different public key cryptographies because public key encryption is the dominating computation in our protocol. The measured delays for different platforms are listed in Table 1, in which Intel SA-1110 is used as the embedded processor in OBUs and RSUs use the other four platforms. It needs to be pointed out that the chosen platforms for RSUs are within the reach of current microprocessors in embedded applications. For example, there are already Pentium-M-based embedded PCs on the commercial market. Although the simulation results depend on the computational capabilities, as we will show later, the probabilistic verification puts OBUs at a more advantageous point than RSUs, making it less favorable for an RSU to cheat.

Table 1. Public Key Encryption Delays for Different Platforms (ms)

Cryptography	Pentium-M 600MHz	Pentium-M 1.7GHz	Xeon 1.8GHz	Xeon 2.8GHz	Intel SA-1110
ecc secp160r1	8.4	4.4	6.1	3.5	51.2
ecc prime192v1	12.4	3.9	5.5	3.2	46.5
ecc secp224r1	16.6	5.4	8.3	4.4	63.6
ecc prime256v1	25.5	8.6	12.7	8.3	178.9
rsa 1024	1	0.3	0.5	0.2	4
rsa 2048	3	1	1.5	0.8	10.7
rsa 3072	6.5	2	3.4	1.6	23.3

The simulated wireless channel is a shared channel among different vehicles. Its channel characteristics are taken from a previously published work on the characteristics of DSRC[23]. We set up a single RSU to authenticate the simulated vehicles. The receiver sensitivity is set to -77dBm according to DSRC standard. The transmission power is set to 17dBm which translates to a transmission range of approximately 300 meters as suggested in [23]. The simulated transmission rate is set at 12mbps.

We run our simulations under different traffic volumes over a period of 4000 seconds. The traffic volume ranges from very light traffic to very heavy traffic as suggested in [16, 24]. During the simulation, we found that the micro-behavior of the vehicle mobility has negligible effects on our results. This is due to the fact that we are simulating the interactions between one RSU and OBUs. To the RSU being simulated, all the OBUs in its service area share the same channel. Thus the movement within its service area does not matter very much. Also, the number of vehicles that are simultaneously within the RSU's service area is bounded due to the necessary physical space between consecutive vehicles. Due to those properties, we generate the traffic volumes in a regular way purely based on the traffic volume data. We expect that this flow models the actual traffic flow for our applications.

Notice that the only comparable scheme with our approach is ring signature. However, the computational cost of ring signature is linear to the level of anonymity, which is more costly than our approach. Due to its apparentness, we do not compare its performance with our approach. Instead, we show the performance gain through the use of the probabilistic anonymity and the extra dimension of adaptivity.

This section is organized in the following way. In Subsection 5.1, we evaluate the response time of our protocol. In Subsection 5.2, the bandwidth used by our protocol is shown. In Subsection 5.3, we investigate how much computation power is required at an RSU to handle different traffic volumes. In Subsection 5.4, we show that the response time is significantly reduced by our adaptive protocol. For all the simulations in this section, the simulation uses Pentium-M 1.7GHz as the platform of the RSU and Intel SA-1110 as the platform of the OBUs except declared otherwise. By default, the cryptography used between the RSU and the OBU is RSA 1024bits. The size of each challenge is 128 bytes. The user confidence in the anonymity is 90% by default.

5.1 Response Time

For each vehicle, we record the time (t_0) at which the vehicle initializes the request, the time (t_1) at which the RSU received the request, the time (t_2) at which the RSU finishes computing all the challenges, the time (t_3) at which all the challenges are received by the vehicle, the time (t_4) at which the vehicle finishes verifying the challenges, the time (t_5) at which the RSU receives the reply, and the time (t_6) at which the vehicle receives the acknowledge. Then we calculate the six durations d_0 to d_5 where $d_i = t_{i+1} - t_i$ for $0 \leqslant i \leqslant 5$. The total communication time spent is calculated as $d_0 + d_2 + d_4 + d_5$

while d_1 is the RSU computation time and d_3 is the OBU computation time.

Fig.5 shows the average times that have been spent for different traffic volumes. All the simulations are run with a group size 100 and a user required anonymity 100. To achieve the required anonymity, the OBU has to verify all the challenges to make sure that the RSU is not cheating. The result is that most time is spent in verifying the challenges by a slower OBU. For a high traffic volume, the communication time and RSU computation time increase slightly due to that the communication channel and the RSU computation resource are shared resources. However, the rate of increase is very small and its effect on the response time is limited.

Fig.6 shows the actual time spent during each phase of the communication. The most time spent in communication is the time used for transmitting the challenges. This is due to a large group size that is requested by the OBUs.

Since the delay incurred by the OBU computation is much larger than the communication delay and RSU computation delay, it clearly favors the use of our probabilistic verification. Even if the computation capabilities of OBUs improve over time, the probabilistic verification puts OBUs at an advantageous point in our protocol, making it less favorable for an RSU to cheat. In the subsequent subsections, we will see the performance improvement of using adaptive privacy.

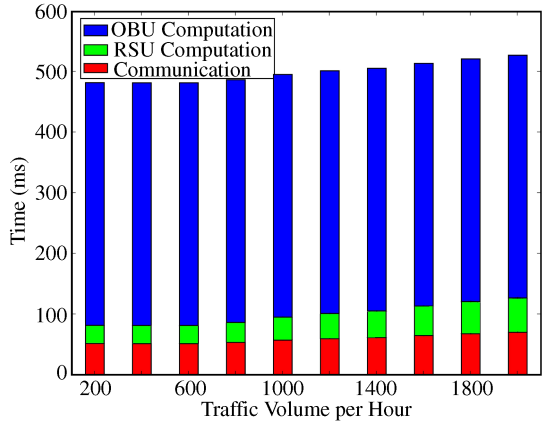


Fig.5. Time spent in different phases for different traffic volumes.

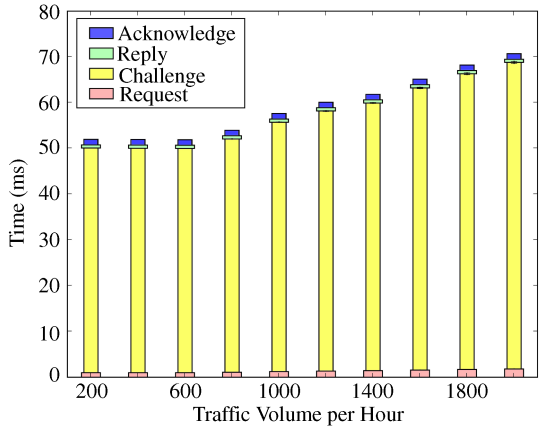


Fig.6. Time spent in communications for different traffic volumes.

5.2 Bandwidth

We also measure the bandwidth used by all the authentications. The consumed bandwidth includes both broadcast and unicast traffic to reflect the occupation of the channel. It can be represented in the following equation.

$$\begin{aligned} C &= Pkt_b + (Pkt_r + Pkt_c + Pkt_y + Pkt_a)Num_v \\ &= Pkt_b + (Pkt_r + Num_c \times Size_c \\ &\quad + Pkt_y + Pkt_a)Num_v. \end{aligned}$$

Pkt_b is the announcement packet by the RSU. Pkt_r is the service request packet from the OBU. Pkt_c is the challenge sent from RSU to OBU. $Size_c$ is the size of a challenge to each member. Pkt_y is the reply packet from OBU to RSU. Pkt_a is the acknowledgment packet from RSU. Num_v is the number of vehicles in the group. The sizes of the packets are listed in Table 2.

The result is shown in Fig.7. Compared with the channel bandwidth 12Mbps, the bandwidth used by the authentication protocol is only a very small portion of

Table 2. Different Packet Sizes (bytes)

Pkt_b	132
Pkt_r	12
$Size_c$	128
Pkt_y	132
Pkt_a	6

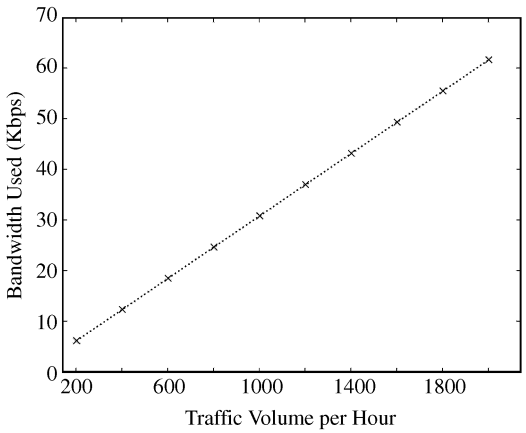


Fig.7. Bandwidth used for different traffic volumes.

it. Even for a high traffic volume of 2000 vehicles per hour, the bandwidth used is only about 60Kbps, less than 1% of the whole bandwidth. This suggests that the authentication protocol will not have significant impact on other applications that need communication bandwidth. Thus the authentication packets can be scheduled with a high priority.

5.3 Capacity

To measure the capacity of an RSU on handling large traffic volumes, we run simulations for different platforms under high traffic volumes. The RSU computation time used for each authentication is shown in Fig.8. The increase of the computation time is almost linear to the traffic volume. The traffic volume of 8000 vehicles per hour is very unlikely in a real network. Given that the traffic volume should have an upper bound and the improvement in computing capacity follows Moore's law, the computation capacity of the RSU is unlikely the bottleneck of our protocol.

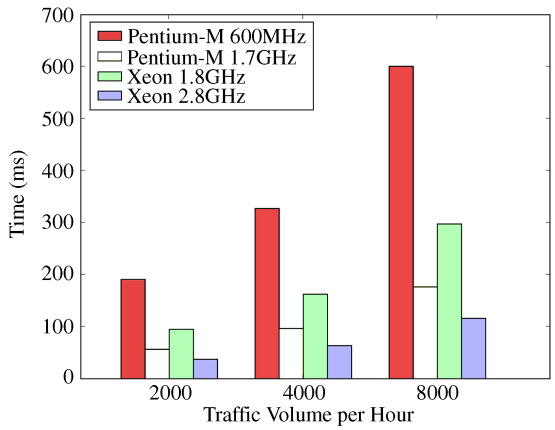


Fig.8. RSU computation time comparison between different platforms with group size 100.

5.4 Adaptivity

We have shown the analytic results in Section 4 that probabilistic verification has significant benefits over a fixed verification scheme. In this section, we show that probabilistic verification enables adaptive privacy-preserving authentications in a road network and significantly improves overall performance. During the simulation, instead of requesting a group size of 100 when the user requires an anonymity of 100, we evaluate two scenarios of adaptive privacy.

In the first scenario, we show that a user can adjust his privacy requirement to get better response. A user is still requesting a group size of 100. However, he adjusts his privacy requirement to anonymity 80. The simulation result is shown in Fig.9. For comparison, the response time without lowering anonymity is also shown. The speed-up is from 2 to 4 times depending on the traffic volume. The speed-up is significant even for a large traffic volume. The result shows that even the privacy is not reduced much, the response time can be significantly improved.

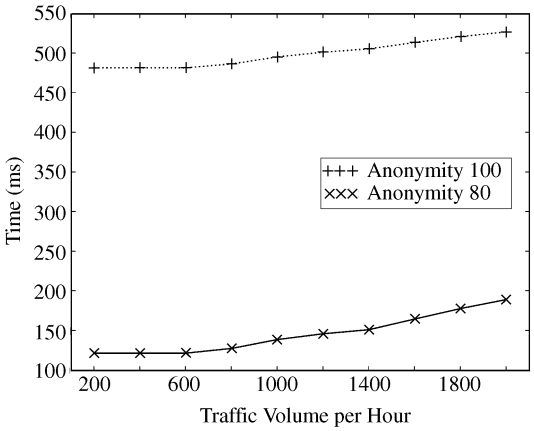


Fig.9. Response time comparison between anonymity 80 and anonymity 100 with group size 100.

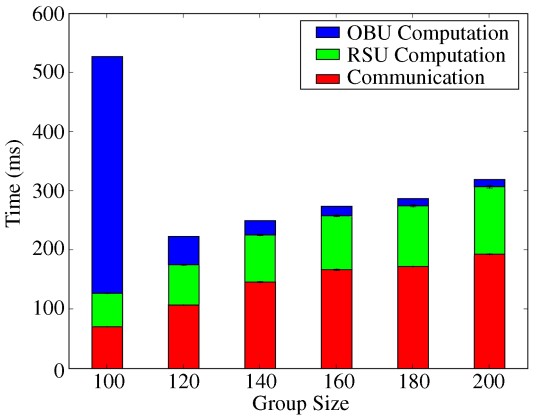


Fig.10. Response time distribution for traffic volume 2000 vehicles per hour with anonymity 100.

In the second scenario, we assume that the user is unwilling to lower his privacy requirement. However, he still wants to improve the response time. We show that by incurring an extra small communication bandwidth, this goal can be achieved. In the simulation, the user still asks an anonymity 100. However, when he requests the authentication, the user specifies a larger group size. The response times for different group sizes requested are shown in Fig.10. The interesting result is that the minimum response time can be achieved with

a small increase on the group size instead of a large increase. The overall response time is cut by more than a half with around 20% increase on the bandwidth. For a large increase, the increased RSU computation time and communication delay reduce the benefits of probabilistic verification.

We are also concerned about the increased bandwidth usage in the second scenario. Fig.11 shows the bandwidth used for different group sizes. The used bandwidth is linear to the group size. Given that an optimal response time can be achieved with a small increase on the group size, the increased bandwidth usage will not undermine our previous conclusion that the authentication protocol does not have significant impact on other applications.

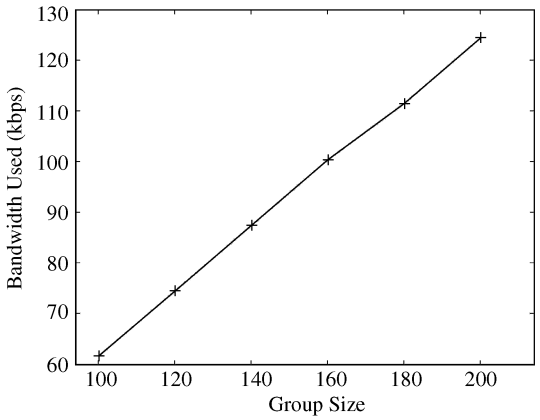


Fig.11. Bandwidth used for traffic volume 2000 vehicles per hour with anonymity 100.

6 Related Work

A lot of work has been done to build vehicular networks, mostly focusing on the design of MAC layer protocols[4], routing protocols[25] based on DSRC[5] and potential applications[26]. However, few efforts address security and privacy issues. Several related efforts are listed as follows.

Attack models and requirements, with some general approaches to preventing these attacks, are described in [27] in detail. The protocol proposed in this paper can be used to prohibit most of these attacks. [28] addresses some security issues in vehicular networks, focusing on system design, but lacks in-depth analysis of privacy protection. Security and privacy of smart vehicles are studied in [6]. This work proposes to use electronic license plates and tamper-proof GPSes to preserve security and privacy, which can be used in our design to strengthen the security and privacy; so their work complements our protocol. Raya and Hubaux also explore the security issues in vehicular ad hoc networks[7]. They analyzed attack models and some concrete attacks, then proposed a set of security protocols for vehicular ad hoc networks. They also designed a key changing algorithm to preserve anonymity and minimize the storage costs of the public keys. However, we use group-based authentication protocol to preserve anonymity, which is different from theirs.

Our authentication protocol is close to a previous group-based approach proposed in [19]. We share the same goal of achieving anonymous authentication based on group information. However, we differ in protocol design. In particular, this paper presents a protocol to support adaptive privacy by making a tradeoff between the privacy and the resource usage. Furthermore, our protocol design is closely integrated with the system design of VII, while theirs is more general. K-anonymity for location privacy is proposed in [16], which anonymizes users at the authentication server so that it is suitable to apply in the *partial trust* case that the RSU is trustable. Our protocol provides adaptive privacy without the requirement of trusting RSUs, i.e., our proposed protocol supports the *zero-trust* model. Ren *et al.* proposed a privacy preserving authentication in [29] that uses blind signature and one-way hash chain to keep privacy. However, their approach does not support adaptive privacy.

Recently, Calandriello *et al.*[15] proposed a pseudonym-based protocol. The protocol uses group signature as the mechanism for a vehicle to generate its own pseudonyms. The pseudonyms can be revealed later under necessary circumstances. Fonseca *et al.*[14] addressed some practical problems in integrating pseudonym-based protocols into VANET. Sun *et al.*[11,12] applied group signature to vehicle-to-vehicle (V2V) authentication and identity-based signature to vehicle-to-infrastructure (V2I) authentication. Group signature-based authentication can be revealed later to provide non-repudiation. Due to the *zero-trust* policy, our protocol does not provide non-repudiation. Instead, our protocol emphasizes the adaptivity of the limited anonymity to the resource usage.

7 Conclusion

In this paper, we analyze the requirements for and challenges of providing security and privacy in VII, and identify the importance of achieving adaptive privacy in the *zero-trust* model. Then, an adaptive, group-based, privacy-preserving authentication protocol is proposed to trade off the privacy and the resource usage. The adaptivity of our protocol gives users more flexible

choices in determining their privacy requirement. Both analytic results and simulation results show that our protocol can be integrated with an RSU to handle a large traffic volume while providing users a large anonymity.

References

[1] Vehicle infrastructure integration. U.S. Department of Transportation, 2006, http://www.its.dot.gov/vii/docs/vii_factsheet.pdf.

[2] Bishop R. A survey of intelligent vehicle applications worldwide. In *Proc. IEEE Intelligent Vehicles Symposium 2000*, Dearborn, MI, USA, Oct. 2000, pp.25–30.

[3] National intelligent transportation systems program plan: A ten-year vision. A Report from Intelligent Transportation Society of America and Department of Transportation. ITSA, DoT, 2002, http://www.itsa.org/itsa/files/pdf/National10YearPlanITSFull.pdf.

[4] Mak T, Laberteaux K, Sengupta R. A multi-channel VANET providing concurrent safety and commercial services. In *Proc. the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Cologne, Germany, Sept. 2005, pp.1–9.

[5] Dedicated Short Range Communications (DSRC) home. DSRC, 2006, http://grouper.ieee.org/groups/scc32/dsrc/.

[6] Hubaux J, Capkun S, Luo J. The security and privacy of smart vehicles. *IEEE Security and Privacy,* 2004, 4(3): 49–55.

[7] Raya M, Hubaux J. The security of vehicular ad hoc networks. In *Proc. the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, USA, Nov. 2005, pp.11–21.

[8] Dötzer F. Privacy issues in vehicular ad hoc networks. In *Proc. Workshop on Privacy Enhancing Technologies*, Dubrovnik, Croatia, May 2005, pp.197–209.

[9] Choi J, Jakobsson M, Wetzel S. Balancing auditability and privacy in vehicular networks. In *Proc. the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, Montreal, Canada, Oct. 2005, pp.79–87.

[10] Sampigethaya K *et al.* CARAVAN: Providing location privacy for VANET. In *Proc. Embedded Security in Cars* (*ESCAR*), Cologne, Germany, Nov. 2005.

[11] Sun X, Lin X, Ho P P. Secure vehicular communications based on group signature and id-based signature scheme. In *Proc. International Conference on Communications* (*ICC*), Glasgow, Scotland, Jun. 2007, pp.1539–1545.

[12] Lin X, Sun X, Ho P P, Shen X. GSIS: A secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, Nov. 2007, 56: 3442–3456.

[13] Guo J, Baugh J, Wang S. A group signature based secure and privacy-preserving vehicular communication framework. In *Proc. the Mobile Networking for Vehicular Environments* (*MOVE*) *Workshop in Conjunction with IEEE INFOCOM*, Anchorage, Alaska, USA, May 2007, pp.103–108.

[14] Fonseca E, Festag A, Baldessari R, Aguiar R. Support of anonymity in VANETs — putting pseudonymity into practice. In *Proc. IEEE Wireless Communications and Networking Conference* (*WCNC*), Hong Kong, China, March 2007, pp.3400–3405.

[15] Calandriello G, Papadimitratos P, Lloy A, Hubaux J P. Efficient and robust pseudonymous authentication in VANET. In *Proc. the Fourth ACM International Workshop on Vehicular Ad Hoc Networks* (*VANET 2007*)*, in Conjunction with ACM MobiCom 2007*, Montreal, Canada, 2007, pp.19–28.

[16] Gedik B, Liu L. Location privacy in mobile systems: A personalized anonymization model. In *Proc. the 25th International Conference on Distributed Computing Systems*, Columbus, Ohio, USA, Jun. 2005, pp.620–629.

[17] Reid D B. An algorithm for tracking multiple targets. *IEEE Transactions on Automatic Control*, Dec. 1979, 24(6): 843–854.

[18] Rivest R L, Shamir A, Tauman Y. How to leak a secret. *Lecture Notes in Computer Science* 2248, 2001, pp.552–565. http://citeseer.ist.psu.edu/rivest01how.html.

[19] Schechter S, Parnell T, Hartemink A. Anonymous authentication of membership in dynamic groups. In *Proc. the Third International Conference on Financial Data Security and Digital Commerce*, Anguilla, British West Indies, Jan. 1999, pp.184–195.

[20] Auto theft key statistics. Insurance Information Institute, 2007, http://www.iii.org/.

[21] GM OnStar System Could Halt Stolen Cars. Associated Press, 2007.

[22] Zeng X, Bagrodia R, Gerla M. GloMoSim: A library for parallel simulation of large-scale wireless networks. In *Proc. Workshop on Parallel and Distributed Simulation*, Banff, Alberta, Canada, 1998, pp.154–161.

[23] Yin J, ElBatt T, Yeung G, Ryu B, Habermas S, Krishnan H, Talty T. Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In *Proc. the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, Philadelphia, PA, USA, Oct. 2004, pp.1–9.

[24] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. ACM MobiSys'03*, San Francisco, CA, USA, May 2003, pp.31–42.

[25] Munaka T, Yamamoto T, Watanabe T. A reliable advanced-join system for data multicasting in its networks. *IEEE Transactions on Intelligent Transportation Systems*, Dec. 2005, 6(4): 424–437.

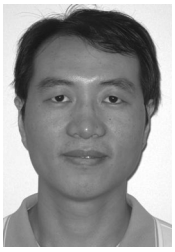
[26] TrafNet: Real-time seattle area traffic conditions over the Internet. University of Washington, 2006, http://www.its.washington.edu/trafnet/.

[27] Aijaz A, Bochow B, Dötzer F, Festag A, Gerlach M, Kroh R. Attacks on inter-vehicle communication systems — An analysis. In *Proc. 3rd International Workshop on Intelligent Transportation* (*WIT 2006*), Hamburg, Germany, March 2006.

[28] Zarki M, Mehrotra S, Tsudik G, Venkatasubramanian N. Security issues in a future vehicular network. In *Proc. EuroWireless 2002*, Florence, Italy, Feb. 2002.

[29] Ren K *et al.* A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular Technology,* 2006, 55(4): 1373–1384.

Yong Xi received the B.E. and M.E. degrees from Beihang University in 1995 and 1998, respectively. He is currently a Ph.D. candidate at Wayne State University. His current research interests include security and privacy in wireless sensor networks and vehicular networks.



Ke-Wei Sha received the B.S. degree from East China University of Science Technology in 2001, and the Master's degree from Wayne State University in 2006. He is currently finishing his Ph.D. degree at Wayne State University and is a visiting assistant professor at Oklahoma City University. His research interests include distributed systems, wireless sensor networks, and vehicular networks, especially in data quality management, system design as well as security and privacy.

Wei-Song Shi is an associate professor of computer science at Wayne State University. He received his B.S. degree from Xidian University in 1995, and Ph.D. degree from the Chinese Academy of Sciences in 2000, both in computer engineering. His current research focuses on mobile computing, distributed systems and peer-to-peer systems, and wireless sensor networks. He has published more than 80 peer-reviewed journal and conference papers in these areas. He is the author of the book "Performance Optimization of Software Distributed Shared Memory Systems" (Higher Education Press, 2004). He has also served on technical program committees of several international conferences, including WWW, ICPP, MASS. He is a recipient of Microsoft Fellowship in 1999, the President Outstanding Award of the Chinese Academy of Sciences in 2000, One of 100 Outstanding Ph.D. Dissertations (China) in 2002, "Faculty Research Award" of Wayne State University in 2004 and 2005, the "Best Paper Award" of ICWE'04 and IPDPS'05. He is a recipient of the NSF CAREER award.

Loren Schwiebert received the B.S. degree in computer science (with a dual major in mathematics) from Heidelberg College, Tiffin, OH, and the M.S. and Ph.D. degrees in computer and information science from the Ohio State University, Columbus, OH. Since 1995 he has been a faculty member at Wayne State University, Detroit, MI, where he is currently an associate professor in the Department of Computer Science and Chair of the Graduate Committee. His research interests include wireless sensor networks, digital forensics, and vehicular networks. He is a member of the ACM, IEEE, and IEEE Computer Society.

Tao Zhang received his Ph.D. degree in electrical and computer engineering from the University of Massachusetts Amherst, USA. He is chef scientist in automotive networking at Applied Research of Telcordia Technologies, Piscataway, New Jersey, USA. He has been directing the R&D program to design the privacy-preserving security system for the US Department of Transportation's Vehicle Infrastructure Integration (VII) initiative, which develops technologies for a national scale automotive networking and applications system. Before joining Telcordia (then Bellcore) in 1995, he worked at Citibank, Lehman Brothers, and Dow Jones/Telerate, where he led strategic planning, design, implementation, and deployment of software systems and networks for global real-time financial data collection, integration, processing, and distribution. Dr. Zhang co-authored the book "IP-Based Next Generation Wireless Networks" published by John Wiley & Sons in 2004. He holds 14 patents, with over 25 more patent applications pending. He serves as an associate editor of the IEEE Transactions on Vehicular Technologies (TVT), and on the editorial board of the Journal of Wireless Networks. He received the 2000 Telcordia CEO Award for most exceptional teams and individuals who have achieved a significant business success. Recently, he has been directing Telcordia's effort on the Vehicle Infrastructure Integration (VII) program sponsored by the US Department of Transportation to develop the security and privacy system for VII.

Appendix

Assume that a group has n members, the RSU uses a subgroup of size s to probe the OBU's identity, and the OBU randomly verifies another m slot, in addition to the private key decryption for obtaining the challenge.

The selection of s slots by the RSU is independent of the selection of m slots verified by the OBU. So we can assume that the s slots are determined and m slots are randomly drawn out of n slots. Among the s slots, one slot corresponds to the OBU. That is to say, there are exactly $s-1$ slots that hold the same challenge value as that for the OBU. The probing is successful when the OBU chooses the m slots out of the $s-1$ slots. The total number of such cases is:

$$C_{s-1}^{m}.$$

However, the total number of ways to choose the m slots out of $n-1$ slots is:

$$C_{n-1}^{m}.$$

So the probability of successful probing is:

$$P = \frac{C_{s-1}^{m}}{C_{n-1}^{m}}. \tag{A}$$