情報保護學會論文誌
第20卷 第4號, 2010. 8

신뢰 RSU 세팅이 필요 없는 VANET 보안통신 기법*

하비[†] , 이쿤, 김범한, 이동훈[‡]
고려대학교 정보경영공학전문대학원

A Secure Communication Scheme without Trusted RSU Setting for VANET*

He Fei[†] , Li Kun, Bum Han Kim, Dong Hoon Lee[‡]
Graduate School for Information Management and Security, Korea University

요 약

근접한 차량으로부터 수신한 브로드캐스트 메시지는 운전자와 승객의 생명과 직간접적으로 연관이 있는 메시지를 포함하고 있기 때문에 VANET에서 보안 통신은 주요 과제 중 하나가 되어 왔다. 이 때문에 보안 통신에 대한 다양한 기법들이 제안되어 왔다. 하지만, 그 기법들의 대부분은, 직접적으로 관리되지 않는 즉 방치된, RSU를 신뢰해야 한다는 가정에 기반을 두고 있다. 본 논문은 RSU를 신뢰할 필요가 없는 보안 통신 기법을 제안하며 사용자의 익명성을 위태롭게 하는 것 없이 서버에 지워지는 부담을 평균적으로 나누기 위하여 그룹핑 기술을 적용하였다. 게다가 본 논문에서는 상대적으로 낮은 하드웨어 성능을 요구하는 보안 요구 사항을 만족시키기 위하여 완전 집합(Complete set)을 설계하였다. 마지막으로 본 논문은 보안 요구사항, 통신 오버헤드, 저장 용량, 그리고 네트워크 성능 측면에서 제안한 기법을 평가하였다.

ABSTRACT

Secure communication has been one of the main challenges in vehicular ad hoc networks(VANET) since broadcast messages from nearby vehicles contain life-critical information for drivers and passengers. So far various secure communication schemes have been proposed to secure the communication in VANET, and they satisfy most security requirements. However most of them need to put trust on roadside units(RSUs), which are usually deployed in unattended area and vulnerable to compromise. In this paper, we propose a secure communication scheme, which does not need to put trust on RSUs. And we adopt a grouping technique to averagely divide the huge burden in the server without jeopardizing the anonymity of users. Moreover we design a complete set of protocols to satisfy common security requirements with a relatively lower hardware requirement. At last, we evaluate the scheme with respect to security requirements, communication overhead, storage overhead and network performance.

Keywords: VANET, secure communication, temporary anonymous certificate

I. Introduction

Vehicular ad hoc networks(VANET) enable vehicles to communicate with each other and roadside units(RSU) by virtue of onboard unit(OBU) equipped in each vehicle and dedicated short range communications(DSRC[1]). With such networks the

* 접수일(2010년 2월 28일), 수정일(1차: 2010년 5월 4일), 게재확정일(2010년 5월 7일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI002113, Car-헬스케어 보안 기술개발]

† He Fei, hefei1986@gmail.com
‡ Dong Hoon Lee, donghlee@korea.ac.kr

safety and efficiency in transportation systems can be improved. According to DSRC, each vehicle should periodically broadcast its routine traffic and safety information[2] which contains its current location, speed, changing of direction or some urgent situation. With such information, the recipient can be well aware of their driving environment and make appropriate decision to avoid traffic accident or jam.

All the attractive functionalities mentioned above should be based on a secure and privacy preserving authentication scheme. Receivers should not only be convinced that the message is intact and fresh, but also be convinced that it really come from the claimed source vehicle. At the same time, the user's personal information, such as the driver's name, license plate, etc, must be protected from leaking out, otherwise the attacker can track the driver's moving history and current location. For the police authority, it should be able to identify the real identity of the sender of any malicious message and stop his further misbehavior. Different from the conventional networks, the hardware resource on OBU is strictly limited and the wireless communication has a higher channel error rate than the one in conventional network, so the security protocols that work well in conventional networks may be no longer suitable for the VANET. In this paper, we are committed to design a secure communication scheme for VANET to solve these problems with a relatively lower hardware requirements on OBU.

1.1 Related Work

Many security protocols for VANET have been proposed. Security issues remain to be solved in VANET are surveyed in [3]. The attack types and a set of security primitives are discussed in [4]. Extensive studies have been reported on inter-vehicle communications(IVC) in [5]. A huge anonymous keys based protocol was proposed in [6], in that scheme each OBU is equipped with a huge number of certified key pairs(denoted as HAB in the following context). The OBU chooses one of them randomly to sign the traffic message in a certain period of time and changes the key pairs in next period of time in order to provide the sender with anonymity. To achieve traceability, the authority keeps all the certified key pairs that each vehicle possesses. In GSIS[7], a group signature technique based scheme(denoted as GSB in the following context) was proposed, it integrates the techniques of group signature[8] and identity based signature (IBS[9]). In GSB the wireless communications are divided into two categories and secured with different approaches: group signature is used to sign the messages launched by OBUs and identity based signature is used to sign the messages launched by RSUs. In [10], the authors proposed a VANET key management scheme, which is based on temporary anonymous certified keys(denoted as TACK in the following context) to achieve anonymous authentication and short revocation list. A conditional privacy preservation protocol(denoted as ECPP in the following context) was proposed in [11]. In ECPP, the privacy is divided into three levels and RSUs are responsible for issuing temporary public key certificates for vehicles.

The above papers respectively addressed most of security problems that VANET encounters with, but they are not perfect. HAB[6] and GSB[7] both fall short in the aspects of requiring a huge storage for anonymous keys and safety message anonymous authentication. GSB[7] and TACK[10] both adopt group signature, which needs a strong computational capacity, however the hardware resource on OBU is strictly limited. GSB[7] and ECPP[11] fall short of putting trust on the RSUs, which are usually deployed in the unattended area and more attractive and vulnerable to compromise.

1.2 Our Contribution

In this paper, we will propose an anonymous authentication protocol that integrates most merits of existing protocols listed in previous subsection.

Most of the existing schemes need to put trust on the RSUs, however the RSUs are usually deployed in unattended area, this weakens the security level of the scheme. In our proposed scheme, the RSU only acts as a message forwarder between sever and vehicle, it does not need to process any sensitive information, consequently there comes an obvious obstruction for such a architecture in VANET, it is the burden for the server. Because there may be a huge number of vehicles in the scheme, the burden for the server could be unacceptable. We adopt a grouping technique, the vehicles are divided into small groups and each group is managed by one of distributed servers(DS), by which the burden of server can be divided averagely without jeopardizing the anonymity of the vehicles.

To achieve the revocation, a revocation list(RL) is used in most of existing schemes. HAB and GSB both use the RL, and they both need a large unacceptable storage space when the size of RL becomes big. In TACK, temporary anonymous certified keys is used to tackle the problem. The temporary anonymous certified keys are also used in our proposed protocol to achieve relative short RL.

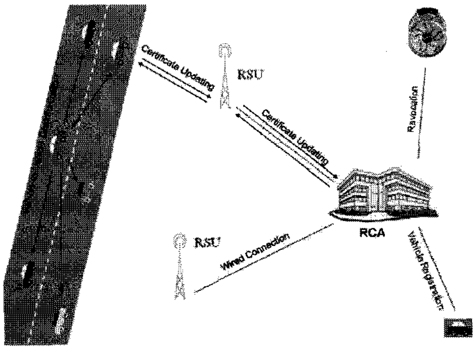
Because of the strict limitation on hardware resource on OBUs, the scheme is designed to use a variant of ECDSA-192[12][13] and keyed-hash function[14] as main cryptographic algorithms, both of them need relatively lower computing resource.

The remainder of the paper is organized as follows. In Section 2, the scheme architecture and some important details will be described, followed by the security analysis, communication overhead analysis and storage overhead analysis in Section 3. We present the simulation in Section 4. Finally we conclude the paper in Section 5.

II. Proposed Scheme

2.1 System Model and Assumptions

Usually VANET hierarchically consists of three layers of entities as shown in Figure 1. The first layer is registration & certificates authority(RCA), which is assumed to be trusted by all parties and it is infeasible for any attacker to compromise. The second layer consists of the roadside units(RSUs), which are usually deployed in unattended area. The RSUs are considered as untrusted entities and wired-connected to the RCA, in proposed scheme the delay between RCA and RSU is assumed to be negligible. According to DSRC, the communication range of RSU and OBU is about 300m, so in the proposed scheme we assume that the RSUs are deployed along the road every 600m to guaran-



(Figure 1) System Model

tee that OBU can update its temporary certified key before it expires at all time. The third layer consists of all the vehicles. We assume that every vehicle is equipped with global positioning system(GPS)[15], an accurate clock and tamper-proof device[16], which can protect the pre-shared sensitive information from leaking out. The number of OBUs in the whole scheme could be up to millions, the number of RSUs depends on the total distance of roads, and there is only one RCA.

2.2 System Notations

The following notations are used to describe the scheme.

RCA: Registration & certificate authority.

G_k: The group id of the k^{th} group.

$N_{\max}$: The maximum number of vehicles in one group.

DS_k: The k^{th} distributed server.

VD_k: The k^{th} vehicle database.

THD_k: The k^{th} temporary id history database.

PK_{id}: The public key of id

SK_{id}: The private key of id

V_i: The i^{th} vehicle with designated equipment

ID_i: The real identity of V_i

ID_{ij}: The j^{th} temporary id of V_i

$ENC_k(m)$: A symmetric-key encryption function on message m using the key k

$DEC_k(m)$: A symmetric-key decryption function on message m using the key k

$HMAC_k(m)$: Keyed-hash message authentication code on message m using the key k

$SIG_{ID}(m)$: Signature on message m with ID's private key

$CERT_{ij}$: The j^{th} temporary certificate of vehicle V_i

LLK_i: Long-live key shared between V_i and RCA

$H(m)$: A cryptographic hash function on message m

$T_{valid-ID_{ij}}$: Valid time for ID_{ij}

$T_{valid-period}$: The alive time for a temporary id

ϵ: A time threshold to check the freshness of messages.

t_{event}: The timestamp of event.

2.3 Scheme Description

2.3.1 RCA Initiation

RCA consists of n distributed servers(DSs), each DS manages a group of vehicles and maintains two databases: vehicle database(VD) and temporary id history database(THD). The number of users in one group is less than $N_{\max}$ in order to keep the time used for database operation small.

Vehicle database. VD keeps the current temporary id, current private key, T_{valid} for current temporary id, last-used temporary id, real id and the LLK. The format of the record in VD is as follows:

$$ID_{ij}||SK_{ID_{ij}}||T_{valid-ID_{ij}}||ID_{i(j-1)}||ID_i||LLK_i$$

Temporary id history database. THD records all the temporary ids that have been used by vehicles and corresponding real id. This database is used for tracing the real identity of any malicious traffic message presented to RCA by police authorities.

2.3.2 Vehicle Registration Phase

At first each vehicle must register at RCA before it can use the VANET system. The registration process is as follows:

1. When the vehicle V_i comes to register, the vehicle is randomly assigned to a

group G_k, in which the number of vehicles is less than $N_{\max}$.

2. RCA redirects the registration request to the DS_k, and V_i submits its real id ID_i to DS_k at $t_{register}$.
3. On receiving the ID_i, DS_k generates a symmetric key as ID_i's long-live key (LLK_i) and an asymmetric key pairs: $PK_{ID_{i1}}$(same with ID_{i1}) and $SK_{ID_{i1}}$ at random. Then DS_k computes the $T_{valid-ID_{i1}}$ by the following equation:

$$T_{valid-ID_{i1}} = t_{register} + T_{valid-period}$$

Then DS_k generates V_i's first temporary certificate by the following equation:

$$CERT_{i1} = SIG_{RCA}(H(T_{valid-ID_{i1}} \| ID_{i1}))$$

4. Then DS_k sends the ID_{i1}, $SK_{ID_{i1}}$, $T_{valid-ID_{i1}}$, G_k and $CERT_{i1}$ to V_i through a secure channel. Then DS_k updates related databases.
5. On receiving the first temporary id and related information, V_i saves ID_{i1}, $SK_{ID_{i1}}$, $T_{valid-ID_{i1}}$, G_k and $CERT_{i1}$ into the tamper-proof device on OBU.

   Vehicle registration phase done.

2.3.3 Certificate Updating Phase

Because the valid period of each temporary certificate is limited, the vehicle needs to update its temporary certificate before it expires. The vehicle can update it with the help of RSUs. The certificate updating process is as follows:

1. V_i sends the certificate updating requesting message(CURM) to the nearest RSU. The format of CURM is as follow:

   $CURM = (ID_{ij} \| t_{send} \| G_k \| HMAC_{LLK_i}(ID_{ij} \| t_{send}))$
2. On receiving the CURM from the V_i, RSU checks the freshness of the message by the following equation:

   $t_{current} - t_{send} < \epsilon$

   If the CURM is fresh, the RSU forwards it to RCA, otherwise abandons it.
3. On receiving the CURM, the RCA forwards it to DS_k.
4. On receiving the CURM, DS_i looks up the vehicle database for ID_{ij}. There are two cases:

Case 1: If the ID_{ij} is found in the “current temporary id” field, DS_k generates a new asymmetric key pairs $PK_{ID_{i(j+1)}}$(same with $ID_{i(j+1)}$) and $SK_{ID_{i(j+1)}}$, then computes the $T_{valid-ID_{i(j+1)}}$ by the following equation:

$$T_{valid-ID_{i(j+1)}} = t_{receive} + T_{valid-period}$$

DS_k generates a new temporary certificate by the following equation:

$$CERT_{i(j+1)} = SIG_{RCA}(H(T_{valid-ID_{i(j+1)}} \| ID_{i(j+1)}))$$

At last DS_k generates the certificate updating message(CUM) and updates related databases. The format of CUM is as following:

$$CUM = (ENC_{LLK_i}(ID_{i(j+1)} \| SK_{ID_{i(j+1)}} \| T_{valid-ID_{i(j+1)}} \| CERT_{i(j+1)}))$$

Case 2: If the ID_{ij} is found in the “last used temporary id” field. It indicates that in last certificate updating session, the vehicle failed to receive the CUM and still used the old temporary id to apply for updating. If this happens, the DS_k needs to do:

Gets the temporary id in “current temporary id” field and the $SK_{ID_{i(j+1)}}$ in private key field, computes a new $T_{valid-ID_{i(j+1)}}$ by the following equation:

$$T_{valid-ID_{i(j+1)}} = t_{receive} + T_{valid-period}$$

Then DS_k generates a new temporary certificate by the following equation:

$$CERT_{i(j+1)} = SIG_{RCA}(H(T_{valid-ID_{i(j+1)}} \| ID_{i(j+1)}))$$

At last DS_k generates the CUM and updates related databases.

5. DS_k sends the CUM to RCA.
6. On receiving the CUM, the RCA forwards it to the original RSU.
7. On receiving the CUM, the RSU forwards it to V_i immediately.
8. On receiving the CUM, the V_i updates the temporary id and related information.

Certificate updating phase done.

2.3.4 Message Authentication Phase

When V_i broadcasts the traffic message M to its neighbors, the message authentication is needed. The message authentication process is as follows:

1. V_i generates a timestamp $t_{broadcast}$ and signs on the message M and $t_{broadcast}$:

$$SIG_{ID_{ij}}(H(M\|t_{broadcast}))$$

Then V_i constructs a traffic message(TM) and broadcasts it to its neighbors.

$$TM=(M\|t_{broadcast}\|SIG_{ID_{ij}}(H(M\|t_{broadcast}))\\ \|T_{valid-ID_{ij}}\|ID_{ij}\|G_k\|CERT_{ij})$$

2. On receiving TM, the recipient needs to do the following steps to authenticate the message.

Step 1. Checks the freshness of the message by the following equation:

$$t_{current}-t_{broadcast}<\epsilon$$

If it is not fresh, abandons the TM.

Step 2. Checks the revocation list to see if the ID_{ij} has been revoked. If it has been revoked, abandons the TM.

Step 3. Verifies the temporary certificate $CERT_{ij}$ with public key of RCA. If it is not valid, abandons the TM.

Step 4. Verifies $SIG_{ID_{ij}}(H(M\|t_{broadcast}))$ with sender's temporary public key (ID_{ij}). If it is valid, accepts M, otherwise abandons it.

Message authentication phase done.

2.3.5 Tracing and Revocation Phase

Given a malicious TM, RCA can identify the vehicle and stop its further misbehavior through the following steps:

1. RCA sends the ID_x to the DS with group number G_k.
2. On receiving the ID_x, DS_k looks up the VD and the THD, gets the corresponding real identity ID_i, puts it into black list and checks the VD to see whether it still has alive temporary certificate. If it still has alive temporary certificate, DS_k constructs a revocation message(RM).

The format of RM is as follows:

$$RM=(\mathrm{ID_x}\|\mathrm{T_{valid-ID_x}}\|\mathrm{SIG_{RCA}}(\mathrm{H}(\mathrm{ID_x}\|\mathrm{T_{valid-ID_x}})))$$

Then DS_k sends the RM and real id(ID_i) to RCA.

3. On receiving the RM and ID_i, DS_k gives ID_i to police authority and forwards the RM to all the RSUs.
4. On receiving the RM, RSUs broadcasts it to the vehicles within its coverage.
5. On receiving the RM, V_i first verifies the signature signed by RCA with RCA's public key, if valid, V_i add the .revoked temporary id ID_x and $T_{valid-ID_x}$ into the revocation list on its OBU.

Tracing and revocation phase done.

2.4 Some Important Details

2.4.1 Countermeasure to Certificate Updating Failure

Proposed scheme provides an efficient mechanism to deal with the certificate updating failure caused by the high transmitting error rate in wireless channel. There are two cases of failure, the solutions for each are as follows:

1. The transmitting error happened to the CURM. If this happens, the RCA can not receive the CURM. The countermeasure is simple, the vehicle just waits for a certain period of time, if it does not get the CUM in the period, it sends the CURM again.

2. The transmitting error happened to the CUM from RCA to the vehicle. It indicates that the RCA indeed received the CURM, generated the new temporary id and sent the CUM to the vehicle, however the transmitting error happened to the CUM and the vehicle failed to receive the CUM. We address this problem with adding a "last used temporary id" field into the vehicle database to records the old temporary id to keep the consistency of vehicle database. The detail has been described in Section 2.3.3.

2.4.2 Reducing Redundant Computation

In some cases, some vehicles may be in the same area in a certain period, so there may be redundant computation on verifying the message sent by the same vehicle. In order to avoid such kind of redundant computation, we propose this optimization. To carry out the optimization we need to add a device into the OBU to record the valid $PK_{ID_{ij}}$ and corresponding $T_{sign-time}$. For instance, we assume V_1 and V_2 are the two vehicles running in the same area in a certain time, when V_i broadcasts a message to its neighbors with using temporary id(ID_{ij}), if the message passes the authentication, its neighbors can save the ID_{ij} and corresponding $T_{valid-ID_{ij}}$. So its neighbors do not need to verify the certificate repeatedly until ID_{ij} expires.

2.4.3 Auto-removal of Expired Records in RL

Each temporary certified key pair has a valid time, if the key pair expires, the user can not use it anymore. As a result the RL does not need to record the revoked temporary id that expires. In proposed scheme, the OBU periodically checks the RL, if any revoked temporary id expires, the corresponding entry can be removed so as to keep RL in proposed scheme small.

III. Analysis

In this section we will do analysis to our proposed scheme with respect to security properties, communication overhead, storage overhead and computation overhead.

3.1 Security Analysis

Authenticity. In the proposed scheme, message authentication is guaranteed through the digital signature signed by the sender with sender's temporary private key, so the adversary can not generate the signature on modified message on behalf of original sender.

Privacy. In the proposed scheme, the user's privacy preserving is guaranteed by the using of LLK and temporary id. The RCA sends the encrypted certificate updating packet to the vehicle, only the vehicle who possesses the LLK in its tamper-proof device can decrypt the packet and get its new temporary id, private key and the corresponding temporary certificate. Then the vehicle uses its new temporary id to send the traffic message to its neighbors, nobody else can identity the temporary id except the RCA.

Short-term linkability. Proposed scheme achieves short-term linkability by using the temporary id, because each temporary id has a life time $T_{valid-period}$, before the certificate updating, the vehicle can't send message with other temporary id.

Long-term unlinkability. Proposed scheme also achieves long-term unlinkability by using the temporary id, one temporary id can only used by one vehicle within a period of time $T_{valid-period}$, after the certificate updating, the vehicle can get a new temporary id and use it to send message. As a result adversaries can no longer link the messages sent by new id with the ones sent with old id. The selection of $T_{valid-period}$ is important, if the $T_{valid-period}$ is small, the unlinkability is better but the burden on DS becomes heavier. If it is big, the long-term unlinkability will be jeopardized. So in proposed scheme, the $T_{valid-period}$ is set to 1 minute, the reason is described in TACK[10].

Traceability and revocation. Proposed scheme provides the traceability and revocation mechanism. For traceability, all the temporary certificates that each vehicle has ever used are kept in the THD, if the police authority wants to get the real identity of the sender of any malicious traffic message, the DS can get the identity by a simple database query operation efficiently. After a vehicle is traced, if it still has any alive temporary id, the RCA can construct a revocation message and send it to all the vehicles running on the road with the help of RSUs.

Putting no trust on RSUs. In most existing papers, the RSUs are usually considered as trusted parties and responsible to process sensitive information. In fact the RSUs are usually deployed in unattended area, it is hard to manage and secure the sensitive information in RSUs, so the property of putting no trust on RSUs should also be considered as an important property.

〔Table 2〕 Comparison of Security Properties

Security Property	Ours	GSB	HAB	TACK
Authentication	Yes	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes
Short-term Linkability	Yes	No	No	Yes
Long-term unlinkability	Yes	Yes	Yes	Yes
Traceability & revocation	Yes	Yes	Yes	Yes
Putting no trust on RSUs	Yes	No	Yes	No

The comparison of security properties between our proposed scheme with other existing schemes are shown in 〔Table 2〕

3.2 Communication Overhead on OBU

There are four types of messages that are communicated in proposed scheme. They are listed as follows(Let $L()$ denote the length in bytes):

Traffic message(TM). The messages broadcasted by a vehicle every certain time. According to DSRC, the interval is 0.1s or 0.3s. Most communication messages in proposed scheme are TMs. The length of TM is as follows:

$$\begin{aligned} L(TM) &= L(M \| t_{broadcast} \| SIG_{ID_{ij}}(H(M \| t_{broadcast})) \\ &\quad \| T_{valid-ID_{ij}} \| ID_{ij} \| G_k \| CERT_{ij}) \\ &= 100+3+48+3+25+2+48 \\ &= 229\ bytes \end{aligned}$$

Certificate updating requesting message(CURM). The OBU needs to send this message to the nearest RSU for applying a new temporary certificate. The length of CURM is as follows:

$$\begin{aligned} L(CURM) &= L(ID_{ij} \| t_{send} \| G_k \| HMAC_{LLK_i}(ID_{ij} \| t_{send})) \\ &= 25+3+2+16 \\ &= 46\ bytes \end{aligned}$$

Certificate updating message(CUM). After receiving the CURM and the generation of new temporary certificate for the applicant, the distributed server generate the CUM, which contains the certificate updating information. The length of CUM is as follows:

$$\begin{aligned} L(CUM) &= L(ENC_{LLK_i}(ID_{i(j+1)} \| SK_{ID_{i(j+1)}} \\ &\quad \| T_{valid-ID_{i(j+1)}} \| CERT_{i(j+1)})) \\ &= 25+24+3+48 \\ &= 100\ bytes \end{aligned}$$

Revocation message(RM). The length of RM is as follows:

$$\begin{aligned} \mathrm{L(RM)} &= \mathrm{L}(\mathrm{ID_x} \| \mathrm{T_{valid-ID_x}} \| \mathrm{SIG_{RCA}}(\mathrm{H}(\mathrm{ID_x} \| \mathrm{T_{valid-ID_x}}))) \\ &= 25+3+48 \\ &= 76\ bytes \end{aligned}$$

3.3 Storage Overhead on OBU

In this subsection we compare the OBU storage overhead of our scheme with two previously reported protocols: HAB[6] and GSB[7]. In the proposed scheme, each OBU stores a public key of the RCA, a anonymous certified key pair together with its anonymous certification issued by the RCA. Because the certified key has a valid period, the revoked temporary id can be removed when it expires, which has been shown in Section 2.4.3. Assume that the number of revoked temporary id in a certain period of time does not exceed $N_{revoked}$, and each record occupies 29 bytes, so our scheme needs about $N_{revoked}$*29+115 bytes in total.

In HAB, assume that the number of the certified key pairs of a vehicle is N_{huge} and the number of revoked vehicles is n, the total storage space needed by HAB is N_{huge}*(25*n+97) bytes. Compared to proposed scheme, the storage space requirement of HAB increases linearly as the number of revoked vehicles increases rapidly.

In GSB, each OBU needs to record one private key issued by the TA, group id and a revocation list, in which n certificate ids and one signature block are saved. The storage space requirement of GSB also increases linearly as the number of revoked vehicles increases. Although it is not that bad like the one in GSB, it is also unacceptable when the number of revoked vehicles is big.

3.4 Computation Overhead on OBU

[Table 3] Comparison Between ECDSA-192 and Group Signature

	ECDSA-192	Group Signature
Security level	80 bits	80 bits
Sign	5e-4 s	1.78e-2 s
Verify	3e-3 s	1.56e-2 s
Signature	48 bytes	151 bytes
Public key	25 bytes	278 bytes
Private key	24 bytes	43 bytes

In this section we compare proposed scheme with three previously mentioned schemes with respect to computation overhead. The computation overhead on OBU depends on the most expensive cryptographic operation it adopts. In proposed scheme, the most expensive cryptographic operation is ECDSA signing&verifying operation. In HAB, the most expensive cryptographic operation is also ECDSA signing&verifying operation. In GSB, group signature is used to authenticate the traffic messages sent by vehicles. In TACK, group signature is used to update temporary certificate. [Table 3] shows that proposed scheme and HAB need less computation resource than GSB and TACK, the outcome is measured on a Centrino machine with clock speed set at 1.5 GHz in [18].

IV. Network Performance

In this section, we evaluate the proposed scheme with respect to network performance. To evaluate the network performance, we simulate our proposed scheme with NS2[17]. In order to achieve relatively real simulation, two road models are used to do the simulation, one is highway model, the other is city model. The density of the vehicles on the road is the main factor that has a major impact on the system performance, it also decides the total number of messages received by each vehicle. We simulate the proposed scheme in the two models to get average loss ratio and transmission delay with different density setting, then compare the proposed scheme with GSB[7] with respect to packet loss ratio.

4.1 Highway Model

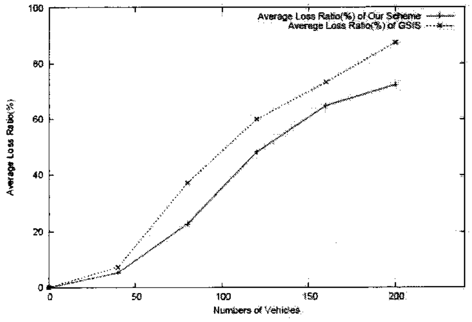
For the highway model, we simulated 8 kilometer long 4-lane highway. The vehicles runs at velocity between 20m/s to 40m/s. The simulation configuration parameters are listed in [Table 4]

According to the simulation results, we found that the transmission delay is not related to the density of vehicles, it is only related to the size of the packet, in our case, when the size of the packet is 229 bytes, the transmission delay is only 2.30ms. The loss ratio of the simulation in highway model is shown in [Figure 2], we can find that the message loss ratio increases as the traffic load increases. When the number of vehicles in the simulation area reaches 200, the packet loss ratio reaches 75%, though this value seems to be big, it is also acceptable because this traffic load is the case where the road is in a severe traffic jam, and in the air there are so many repeated messages sent by vehicles. And in most cases there are usually about 50 vehicles in the same area, so the packet loss ratio 20% is acceptable. The [Figure 2] also shows that the our scheme has lower packet loss ratio than the one in [7] in highway model.

[Table 4] Simulation Configuration for Highway Model

Parameter	Value
Simulation area	9200m*820m
Communication range	300m
Simulation time	100s
Channel bandwidth	7Mbs
Packet size	229 and 301 bytes
Packet interval	0.1s

[Figure 2] Average Loss Ratio in Highway Model



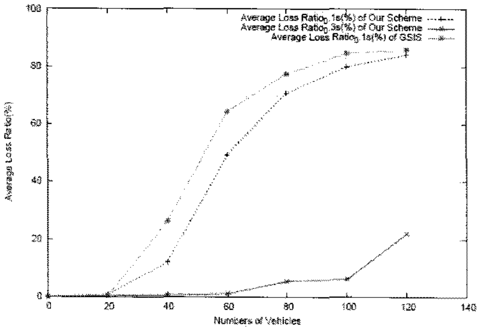
[Table 5] Simulation Configuration for City Model

Parameter	Value
Simulation area	400m*400m
Communication range	300m
Simulation time	100s
Channel bandwidth	7Mbs
Packet size	229 and 301 bytes
Packet interval	0.1s and 0.3s

4.2 City Model

For the city model, we simulated a 400m*400m city area, In this model, the vehicles are dense and the average velocity of vehicles is less. The simulation configuration parameters are listed in [Table 5]

In city model, the transmission delay is the same with the one in highway model. Average loss ratio in city model is shown in [Figure 3], we can find that the message loss ratio increases higher as the traffic load increases. when number of vehicles reaches 120, the packet loss ratio reaches 80%, which is unacceptable. In the city, most of the time the density of vehicles is big, so the packet loss ratio will be too high to tolerate. The solution is prolonging the interval of traffic messages, and the simulation shows that if traffic message interval is set to 0.3s,



(Figure 3) Average Loss Ratio in City Model

the packet loss ratio can be significantly reduced to about 20% in the densest case.

V. Conclusions

In this paper, we have proposed an anonymous authentication scheme for VANET. Based on the temporary certificated keys, the proposed scheme only needs a small storage space for the revocation list. The RSUs are usually deployed in unattended area and vulnerable to compromise, for achieving stronger security level, the proposed scheme does not need to put trust on RSUs. We also adopted a grouping technique to averagely divide the burden in the RCA without jeopardizing the anonymity of the users. And the proposed scheme enables recipient to authenticate the traffic messages, at the same time the anonymity of sender can be preserved. If any vehicle is found to send malicious traffic message, the authority can identify it and stop its further misbehavior.

For future work, we intend to study how to determine the maximum number of vehicles in one group to achieve the optimal tradeoff between performance and cost.

References

〔1〕 Dedicated short range communications (DSRC), 〔Online〕.Available:http://grouper.ieee.org/groups/scc32/dsrc.index

〔2〕 U.S. Department of Transportation, National highway traffic safety administration, Vehicle Safety Communications Project, Final Report, Apr. 2006.

〔3〕 F. Dotzer, "Privacy issues in vehicular ad hoc networks," Privacy Enhancing Technologies, Lecture Notes in Computer Science, Springer Berlin/Heidelberg, pp. 197-209, Mar. 2005.

〔4〕 B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proceedings of HotNets-IV, pp. 1-6, Nov. 2005.

〔5〕 J. Luo, J.P. Hubaux, "A survey of inter-vehicle communication," Technical Report IC/2004/24, EPFL, Lausanne, switzerland, pp. 1-12, Mar. 2004.

〔6〕 M. Raya and J.P. Hubaux, "The security of vehicular ad hoc networks," in Proc. 3rd ACM Workshop Security Ad Hoc Sensor Networks SASN'05., Alexandria, VA, pp. 11-21, Nov. 2005.

〔7〕 X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications," IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456, Nov. 2007.

〔8〕 D. Chaum and E..V. Heyst, "Group signatures," in Advances in Cryptology-EUROCRYPT 1991, LNCS 547, Springer-Verlag, pp. 257-265, Apr. 1991.

〔9〕 A. Shamir. "Identity-based cryptosystems and signature schemes," Advances in Cryptology -Crypto 4, LNCS, Vol. 196, Springer-Verlag, pp. 47-53, Mar. 1985.

〔10〕 A. Studer, E. Shi, F. Bai and A. Perrig, "TACKing together efficient authentication, Revocation, and Privacy in VANETs", Carnegie Mellon CyLab, Tech. Rep, pp. 1-9, Jul. 2008.

〔11〕 R. Lu, X. Lin, H. Zhu, P.H. Ho, and X.

Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in Proceedings of the IEEE International Conference on Computer Communications, Phoenix, Arizona, pp. 1903-1911, Apr. 2008.

〔12〕 ANSI X9.62. Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA), American National Standards Institute, pp. 16-31, 1999.

〔13〕 B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, 2th Ed., Wiley Computer Publishing, pp. 494-495, 1996.

〔14〕 Information Technology Laboratory, National Institute of Standards and Technology, "FIPS PUB 198: the keyed-Hash message authentication code," pp. 1-12, Jul. 2002.

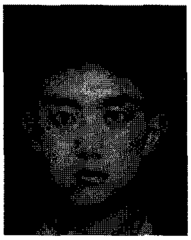
〔15〕 Global positioning system, 〔Online〕. Available: http://www.gps.gov/system/gps

〔16〕 R. J. Anderson,"Security engineering: a guide to building dependable distributed system, John Wiley & Sons, Inc, Wiley Computer Publishing, pp. 277-304, 2001.

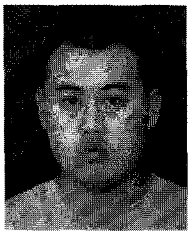
〔17〕 The Network Simulator 2, 〔Online〕. Available: http://www.isi.edu/nsnam/ns/

〔18〕 G. Calandriello, P. Papadimitratos, A. Lloy and J.-P. Hubaux. "Efficient and robust pseudonymous authentication in VANET," In Proceedings of the Workshop on Vehicular Ad Hoc Networks(VANET), pp. 19-28, Oct. 2007.

〈著者紹介〉

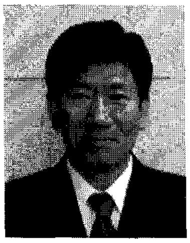


He Fei 학생회원
2008년 7월: Harbin Institute of Technology 졸업
2008년 9월~현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 VANET 보안, 키 교환



Li Kun 학생회원
2008년 7월: Harbin Institute of Technology 졸업
2008년 9월~현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 VANET 보안, 키 교환

김범한 (Bum Han Kim) 학생회원
2004년 2월: 숭실대학교 수학과 졸업
2006년 2월: 고려대학교 정보보호대학원(공학석사)
2006년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 정보보호, VANET, 모바일 보안



이동훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 졸업(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학석사)
1992년 5월: Oklahoma University 전산학 대학원(공학박사)
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, 키 교환, 익명성 연구, PET 기술