Journal of Computer Science 9 (8): 981-989, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.981.989 Published Online 9 (8) 2013 (http://www.thescipub.com/jcs.toc)

ON-THE-FLY KEY GENERATION FOR AN EFFICIENT ROAD SIDE UNITS BASED AUTHENTICATION IN VEHICULAR NETWORKS

[1]Ashraph Sulaiman, [2]S.V. Kasmir Raja and [3]Sung Han Park

[1]Department of Computer Science, National University of Rwanda, Huye, Rwanda
[2]Department of Computer Engineering, SRM University, Chennai, India
[3]Department of Computer Engineering, Hanyang University, Seoul, South Korea

Received 2013-05-26; Revised 2013-06-21; Accepted 2013-07-04

ABSTRACT

Obtaining efficient security without compromising privacy is a primary issue in vehicular communication. Though many counterparts proposed solutions in this regard, accommodating scalability, security and traceability altogether is a difficult task due to the contradictions between these qualities. Some of the previous studies suggests RSU based authentication to address the above issues, while others propose independent OBU authentication. In either scheme, any one of the entities is overloaded during key generation and verification processes. The proposed scheme addresses these issues, by distributing the workload between OBUs and RSUs to outperform other protocols. We propose a novel scheme, in which OBUs generate short-lived public keys on the fly and other vehicles can verify them with the help of RSUs. This protocol also admits certificate-less authentication, in addition to aggregated signature verification. Therefore, the total verification time can be drastically reduced in the proposed scheme. We analyze the proposed protocol significantly to demonstrate its efficiency.

Keywords: VANET, Privacy, Security, Traceability, Pseudo-Id, Signature Verification

1. INTRODUCTION

Vehicular Networks (VANETSs) are established to enhance road safety, traffic management and infotainment facilities. In VANET, each vehicle is equipped with an On Board Units (OBUs) to communicate with other vehicles, Road Side Units (RSUs) that are located on the roads and the Trusted Authority (TA) to register RSUs and OBUs. According to (USDT, 2006) OBUs frequently broadcasts routine traffic related messages with information about its position, current time, direction, speed, acceleration/deceleration, traffic events. This helps the vehicle to be warned with critical situations such as accidents, traffic jams.

Though this communication helps the driver community, it has a critical side effect of privacy. Some studies (Raya and Hubaux, 2005; 2007) proposed pseudonym based approach to solve this problem. Generation of pseudonyms by the TA or RSUs is not an issue with their high computation and storage capacity. However, the computation cost of OBUs grows linearly with the traffic density. Some studies suggests RSU based authentication to reduce the burden of vehicles, while others propose independent OBU authentication. Both the schemes suffer with scalability and message loss problems, as any one entity (OBU or RSU) is solely responsible for key generation and/or verification. The proposed scheme addresses these issues by allowing both OBUs and RSUs to contribute in authentication process.

2. RELATED WORKS

Many studies have been reported on the security and privacy-preservation issues for VANETs proposed by several authors (Raya and Hubaux, 2007; Lin *et al*., 2007; Zhang *et al*., 2008a; Ren *et al*., 2006; Lu *et al*.,

Corresponding Author: Ashraph Sulaiman, Department of Computer Science, National University of Rwanda, Huye, Rwanda

2008). They can be grouped into three categories. First category is based on a huge number of pseudo-anonymous key based (HAB) protocols proposed by several authors (Raya and Hubaux, 2007; Lin *et al*., 2008; Mak *et al*., 2005; Xu *et al*., 2007; Xi *et al*., 2007; 2008). Though this is a straightforward solution, this method requires each OBU has to take large storage space to store a number of anonymous key pairs.

The second category is based on Group Signature (GSB), which was first introduced by Chaum and VenHeyst (1991). This allows a group member to sign messages anonymously on behalf of the group. In case of a dispute, the group manager can reveal the identity of a signer. According to Xiong *et al*. (2010) although the group signature can achieve anonymity on conditional privacy preservation, the time for message verification grows linearly with the number of revoked vehicles. Lin *et al*. (2008) propose an efficient security protocol called GSIS. With this protocol, only a private key and group public key are stored in the vehicle and the messages are signed according to the group signature scheme without revealing any identity information to the public. However, the verification of group signature requires at least two pairing operations, which may not be scalable when the density of traffic is increased. Finally, Calandriello *et al*. (2007) proposed a hybrid approach by combining the pseudonym and the group signature schemes. However, this approach suffers with the same drawbacks.

The third category employs the RSUs to assist message authentication. Lu *et al*. (2008) proposed a protocol called ECPP, in which the RSU issues only an ephemeral certificate for valid vehicles at the time of authentication to eliminate the certificate requirement and the RL. In RAISE, Zhang *et al*. (2008a) employed RSUs to authenticating messages. Compared to the solutions previously mentioned, this scheme enables lower computation and communication overheads for each vehicle. Also, Zhang *et al*. (2008b) introduced IBV scheme, in which multiple signatures can be batch verified instead of one by one. Therefore, the signature verification speed improved significantly and alleviated the computational workload of the RSUs. By generating distinct pseudo identities and the corresponding private keys for signing each message with a tamper-proof device, privacy regarding user identity and location of the vehicles can be protected. However, this scheme requires additional hardware to be installed on OBUs to generate pseudo identities.

However, the verification process of most of the protocols solely depends either on OBUs or on RSUs, which leads to scalability issues when the traffic density goes high. In order to address this downside, we propose this scheme to employ both RSUs and OBUs to work together for the key generation and verification processes, in order to distribute the workload between the two. Thus, this scheme achieves a better performance comparatively to other counterparts even in a high traffic situation.

3. SYSTEM MODELS AND PRELIMINARIES

3.1. System Model

VANET architecture consists of three entities as in **Fig. 1**: (1) the Trusted Authority (TA), who is in-charge for the registration of RSUs and OBUs, (2) the RSUs at the roadside, that act upon the commands of TA and (3) the vehicles equipped with OBUs in order to communicate with other vehicles.

3.2. System Requirements

As any other VANET system, we assume that our system fulfills the following requirements:

- Anonymous Authentication: From the message senders' perception, leaking their privacy information such as Real ID (RID) of the vehicle is unacceptable
- Unlink ability and Traceability: Any recipient cannot link two or more messages sent by a vehicle to other vehicles. On the other hand, the authorities should be able to trace the sender of the message by mapping the message with the real identity of the sender in case of any liability investigation
- Scalability and Low overhead: Any application of the vehicular networks must be scalable to a large network. The computation and communication overhead increases linearly with the number of vehicles in the network

3.3. Bilinear Pairing

Since bilinear maps are the basis of our scheme, we briefly introduce them here. Let G_1, G_2 be the cyclic additive and multiplicative groups of same prime order q. Let P be the generator of G_1. An admissible bilinear map is a map $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ satisfying the following properties:

- Bilinearity: $\forall a, b \in G_1$ and $\forall a, b \in Z_q$, $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$
- Nondegeneracy: $\hat{e}(a,b) \neq 1_{G1}$
- Computability: $\exists$an algorithm to $\hat{e}(a,b)$, $\forall (a,b) \in G_1$

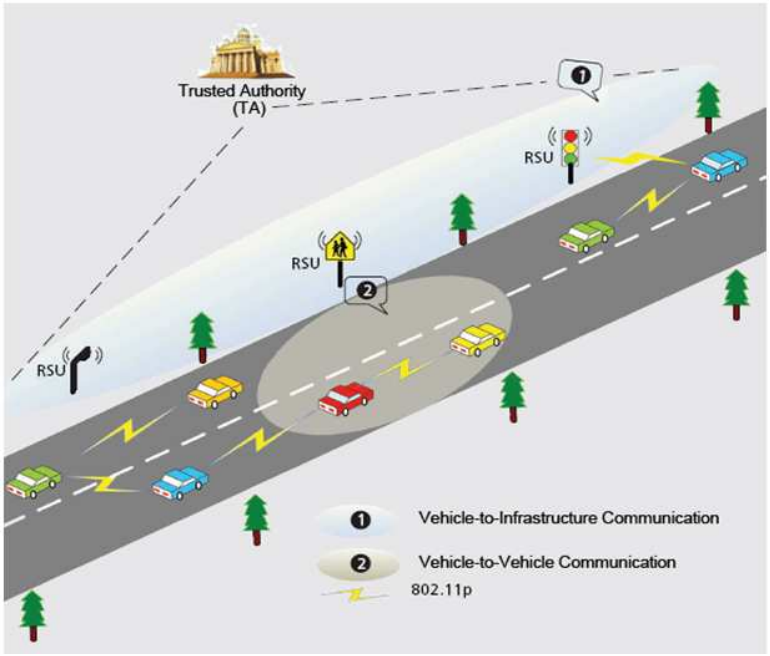

Fig. 1. System model

Table 1. Notations

Notation	Description
S	Secret between RSU and its OBUs
V_x	Thex-th vehicle
R	The RSU
PK^{V_x}	Long term public key of V_x
sK^{V_x}	Corresponding private key of PK^{V_x}
T_{exp}	Time expiry
$Cert_{TA}[PK^{V_x}]$	TA's certificate on PK^{V_x}
PID^{V_x}	Short-lived pseudo-id of V_x
PK^R	Public key of RSU
sk^R	Corresponding private key of PK^R
K_{ss}	Session key between V and RSU
h(.)	A one way hash function such that SHA-1 (Eastlake and Jones, 2001)
H(.):	Hash function such as $H:\{0,1\}^* \rightarrow G_1$(Sweeney, 2002)

Such bilinear map êcan be constructed by modified Weil (Boneh and Franklin, 2001) or Tate paring (Miyaji *et al*., 2001) on elliptic curves.

4. PROPOSED SCHEME

4.1. System Initialization

All the OBUs and RSUs must register themselves with the TA before they join in the VANET. The TA is in-charge of checking the vehicle's identity and to provide a long-term public/private key pair for each vehicle and to set up the system parameters $\{G_1, G_2, q, P\}$ for RSUs and OBU. Rests of the notations are listed in **Table 1**.

4.2. Short-Lived Key Pair Generation

Firstly, RSU (hereafter we say R) randomly chooses $s \in Z_q$ as a common secret between the vehicles in its range and computes $Q = sP$. Also, RSU is responsible to choose a distinct Pseudo-ID (PID) for each vehicle when it comes into its communication range. The detailed working of our protocol is as follows.

At regular intervals, R broadcasts hello messages. When V_x enters into R's proximity, it detects the hello message. Immediately, V_x sends its $Cert_{TA}[PK^{V_x}]$, signed by TA and a random number $r1 \in Zq$ to R, to initiate the mutual authentication process. After authenticating PK^{V_x}, from $Cert_{TA}[PK^{V_x}]$, R chooses r2 as its share to establish a shared session key between $V_x$and itself. This process can be achieved through Diffie and Hellman (1976) key agreement protocol. Besides, R chooses a unique PID for V_x and sends $\{r2||\{PK^{V_x}||T_{exp}||s||Q||r2\}E_{Kss}\}$, where E_{Kss} is encryption using K_{ss}.

With this PID^{v_x}, V_x can now generate anonymous short-lived key pairs on the fly in order to send traffic related messages to other vehicles. In our scheme, OBU's generate these key pairs (U and v respectively) randomly from the given Pseudo-IDs (PID), based on ID based cryptography (Sha *et al*., 2006). Each U is composed of U_1 and U_2. This U_1 and U_2 are the cipher texts of Elgamal (1985) encryption algorithm. Similarly, each private key v consists of v_1 and v_2. Generation of these keys pairs can be detailed in algorithm 1.

Algorithm 1: On-the-fly generation of short-lived public/private keys by the OBUs

Input: PID^{v_x} obtained from RSU

Output: Short-lived anonymous key pairs U^{v_x} and v^{v_x}

i. Computes the short-lived public key U^{V_x} as:

$$U_1^{V_x} = PID^{V_x}\ aP$$

$$U_1^{v_x} = h\left(PID^{v_x}\right) \oplus H\left(PID^{v_x}\ aQ\right)$$

where, a is a random nonce, $\oplus$ is an XOR operation

ii. Computes the corresponding public key vas:

$$v_1^{v_x} = sU_1^{v_x}$$

$$v_1^{v_x} = sH\left(U_1^{v_x} \| U_2^{v_x}\right)$$

In order to generate unique key pairs, V_x changes the random nonce each time it generates a short-lived public/private key.

4.3. Signature Generation

When a vehicle V_x wants to send message M, it generates a short-lived key pair as in algorithm1. It then computes a signature 'σ^{v_x}' on M using the short-lived private key $v^{v_x} = (v_1^{v_x}, v_2^{v_x})$ in such a way that $\sigma^{v_x} = v_1^{v_x} M + v_1^{v_x}$ After that V_x sends $\{U^{v_x} \| M \| TS \| \{Uvx \| M \| TS\}\sigma^{v_x}\}$ to other vehicles. For sending subsequent messages V_x changes its short-lived key pairs by choosing a distinct random nonce 'a'.

4.4. Aggregated List of Pseudo-IDs Agree

Meanwhile, R periodically broadcasts an aggregated list of issued pseudo-id hashes $h_{aggr} = \{h(PID^1), h(PID^2) \ldots h(PID^n)\}$ to the vehicles in its communication range. This list eliminates the certificate overhead. For this purpose, R first hashes the PIDs that are not expired, aggregates them all and signs the aggregated PIDs using sk^R and sends out the signed list $h_{aggr} \| (h_{aggr})_{sk}{}^R$. Each time R issues a Pseudo-ID (PID) to a new vehicle, it appends the new PID in its aggregated list. Similarly, when a PID reaches T_{exp}, it will be cut off from the list. In case a vehicle remains in same R even after the T_{exp} of its PID, it can continue participating in the communication by requesting a new PID from R using K_{ss}.

4.5. Verification

4.5.1. Aggregated Hash Verification

When a vehicle receives messages sent by the other vehicles, the receiver verifies the authenticity of the short-lived public keys from the aggregated pseudo-id hashes published by the RSU's periodically. For this ground, the receiver first computes the pseudo-id hash $h\left(PID^{v_x}\right)$ of a short-lived public key $U^{v_x} = U_1^{v_x} + U_2^{v_x}$ as follows Equation 1:

$$\begin{aligned} &= h\left(PID^{v_x}\right) \oplus H\left(PID^{v_x} aQ\right) \oplus H\left(sPID^{v_x} aP\right) \\ &= h\left(PID^{v_x}\right) \oplus H\left(PID^{v_x} aQ\right) \oplus H\left(PID^{v_x} aQ\right) \\ &= h\left(PID^{v_x}\right) \end{aligned} \quad (1)$$

After extorting the pseudo-id hash $h\left(PID^{v_x}\right)$ from the short-lived public key U^{v_x}, it compares the $h\left(PID^{v_x}\right)$ in the RSU list for its existence.

4.5.2. Batch Signature Verification

Once the receiver confirms the genuineness of the pseudo-ids of all received messages through the aggregated list of pseudo-id hashes, it undergoes verification of signatures for the corresponding short-lived public keys. The authentication of a signature in a message can be carried out using the short-lived public key U of the sender attached in the message. With the system public parameters $\{G_1, G_2, q, P\}$ assigned by the TA and the parameters $\{s, Q\}$ obtained from RSU, the receiving vehicle verifies the signature of the sender V_x as below Equation 2:

$$\begin{aligned} &\hat{e}\left(\sigma^{v_x}, P\right) \\ &= \hat{e}\left(v_1^{v_x} M + v_2^{v_x}\right) \\ &= \hat{e}\left(v_1^{v_x} M, P\right)\hat{e}\left(v_1^{v_x} P\right) \\ &= \hat{e}\left(sU_1^{v_x} M, P\right)\hat{e}\left(sH\left(U_1^{v_x} \| U_2^{v_x}\right)\right), P) \\ &= \hat{e}\left(sP, U_1^{v_x} M\right)\hat{e}\left(sP, H\left(U_1^{v_x} \| U_2^{v_x}\right)\right) \\ &= \hat{e}\left(Q, U_1^{v_x} M + H\left(U_1^{v_x} \| U_2^{v_x}\right)\right) \end{aligned} \quad (2)$$

Since we employ batch verification in our scheme, a receiver can collectively verify n distinct messages from n distinct vehicles once in every 300 ms. If the receiver receives σ^1, σ^2 …σ^n, the signature son the messages M^1, M^2 …M^n with their public keys U^1,U^2….U^n then, those signatures are valid if the following Equation 3 holds:

$$\hat{e}\left(\sum_{i=1}^{n}\sigma\right) \quad (3)$$

4.6. Additional Storage Requirement

Considering the storage requirement, our protocol requires each OBU to store the aggregated list of pseudo-id hashes published by the RSU periodically. However, this may require a small amount of storage capacity, as this list would not grow long, since the expired pseudo-id will be erased incessantly from the list by the RSU.

5. ANALYSIS AND EVALUATION

5.1. Security Analysis

Claim 1: Privacy Preservation and Anonymous Authentication is Achieved

Proof

The RSU can authenticate vehicle V_x through its long-term public key PK^{V_x}, since it is signed by TA's private key. By this way, the real identity of the vehicle is preserved within TA. The short-lived public keys that are used for sending messages are generated from a pseudo-id given by the RSU, that has no trace of this long-term public key. Even if the RSU is hacked by any high level attacks, the real id of a vehicle cannot be revealed from the RSU. In terms of anonymous authentication, RSUs periodically broadcast the aggregated list of valid pseudo-ids signed by its private key sk^R to the vehicles in its range. Therefore, a vehicle can trust a public key if its pseudo-id hash extracted from its public key is present in the aggregated pseudo-id hash of RSU. This shows that, claim 1 is correct.

Claim 2: The Anonymity of the Message Originator and Traceability by the Authorities is Assured

Proof

The short-lived anonymous public key U is computed in such a way that U_1 = PIDaP, U_2 = h(PID)⊕H(PIDaQ) where, 'a' is a random number which would be changed by the vehicle for every different messages. This guarantees a unique short-lived public key each time. Moreover, the pseudo-id of a vehicle PID cannot be retrieved from its hash h(PID) because of the irreversible property of one-way hash chain. Therefore, a receiver cannot link any two short-lived public keys that are generated from the same PID. In case of any dispute, the RSU first fetch the pseudo-id hash in the accused message in order to find the real PID value of the message sender. Later, it extracts the long-term public key of the responsible vehicle and submits it to the TA for penalty. Therefore, claim 2 is correct.

Claim 3: Scalability and Low Verification Overhead is Guaranteed

Proof

In the proposed protocol, a public key certificate is not required as the public keys can be authenticated form the list of aggregated pseudo-id hashes published by the RSU. Though this requires the RSU's signature in the list to be verified, it is one signature shared for *n* messages. Therefore, our protocol dramatically reduces verification overhead and improves the scalability of the system. This confirms that claim 3 is correct.

5.2. Performance Evaluation

5.2.1. Verification Delay

We evaluated and compared our protocol with the following schemes. ECDSA proposed by Boneh *et al.* (2001) BLS proposed by Boneh *et al.* (2003) and GSIS proposed by Choi *et al.* (2011). Here, ECDSA is the traditional PKI based scheme, BLS and GSIS are group based, group and identity based signature schemes respectively. Considering the time to perform one pairing operation T_{pair}, one point multiplication over elliptic curve cryptography T_{mul}; we used the experiment of Scott (2007) with an MNT curve of embedding degree k = 6 and 160 bit q simulated on an Intel Core 2 Duo @ 3 GHz machine and attained the values for T_{pair} = 4.5 and T_{mul} = 0.6 ms.

As depicted in **Table 2**, we calculated the time to sign and verify a single message and n messages. ECDSA uses one T_{mul} operations to sign and 4 times T_{mul} operations to verify a single message. During message verification, for n messages, it requires n times operations as that of single message verification. BLS uses one T_{mtp} one T_{pair} per signing and 4 times pairing and 2 times point multiplication operations to verify a single message. While on the other hand, for verifying n messages, it requires $(2n+2)T_{pair}+2nT_{mtp}$ operations. This is because BLS performs aggregated verification. GSIS is closer to BLS but does not use T_{mtp} operation. Rather, $3T_{pair}+9T_{mul}$ is required during signing a single message and two additional pairing and one reduced multiplication operations are needed for verifying a single message.

Table 2. Comparison of signing and verification speed

	Signing		Verification	
Protocol	1 message	n messages	1 message	n messages
ECDSA	T_{mul}	n T_{mul}	$4T_{mul}$	$4nT_{mul}$
BLS	$T_{mul} + T_{mtp}$	n T_{mul}+ n T_{mtp}	$4T_{pair} + 2T_{mtp}$	$(2n + 2)T_{pair} + 2n\ T_{mtp}$
GSIS	$3T_{pair} +9T_{mul}$	$3nT_{pair} +9nT_{mul}$	$5T_{pair} + 8T_{mul}$	$5nT_{pair} + 8n\ T_{mul}$
Our Protocol	T_{mul}	n T_{mul}	$4T_{pair} + T_{mul} + T_{mtp}$	$4T_{pair}$ + n T_{mul} +n T_{mtp}

For n messages, signing and verification in GSIS requires an equivalent of n times operations with its single message signing and verification time respectively. Our protocol requires similar time as that of ECDSA in signing messages. For verification, our protocol requires $4T_{pair}$, in addition to one T_{mul} and one T_{mtp} operations. This is because, in the total $4T_{pair}$ operations, $2T_{pair}$ remains the same for batch verifying n signatures and another $2T_{pair}$ is for the verification of the ECDSA signature of the RSU that comes along with the list of aggregated pseudo-id hashes, which is one for n messages.

Figure 2 illustrates the message verification delay of the various schemes ECDSA, GSIS and BLS compared with our protocol. The verification delay of GSIS and BLS is higher, when compared to the verification time of ECDSA and our protocol. GSIS starts losing the messages, when the number of messages increases over 10 within 300ms. BLS takes a similar time, as GSIS when number of messages are 50 to verify. ECDSA verifies around 125 messages in 300ms. Our protocol verifies closely twice the messages as verified by ECDSA within the same 300ms time interval.

5.2.2. Communication Overhead

To measure the communication overhead of our protocol, we evaluated our protocol using ns-2 the network simulator, simulation with the parameters shown in **Table 3**.

Our protocol is compared with the ECDSA, BLS and GSIS for the communication overhead occurred due to the cryptographic operations used in the schemes. ECDSA, BLS and GSIS schemes use a certificate of 125 bytes along with their signature costs. 181, 146 and 184 are the additional communication overhead for the above schemes respectively. Since our protocol uses a certificate less communication, it requires an additional overhead of only 42+21+(56/n)bytes, in which 42 bytes are for the short-lived public key and 21 bytes is for its corresponding signature. An additional overhead of 56 bytes is required for the RSU's ECDSA signature in the list of pseudo-id hashes that are periodically by the RSU. However, these 56 bytes would be shared for n messages, as the RSU aggregates all the pseudo-id hashes into one list. Therefore, a total of 63+(56/n) bytes are required as the overall communication overhead in our scheme.

Figure 3 explains the communication overhead all protocols when the vehicle density increases. The simulation time is 1 min; with the vehicles range proposed up to 300 and the communication overhead is measured in megabytes. We also assumed that, RSUs broadcasts the list of aggregated pseudo-id hashes periodically with a time interval of 10ms and vehicles with the interval of 300ms. ECDSA and GSIS occupy a similar overhead and bounce 10 MB when the number of vehicles is more than 275.

Communication overhead of BLS is slightly less than ECDSA and GSIS schemes and consumes slightly over 8 MB, when 300 vehicles in range. Our protocol requires less than the half of the overhead of BLS when the communication is between 300 vehicles and a RSU.

5.2.3. Message Loss Ratio

We evaluated the message loss ratio of our protocol using ns-2 with the parameters shown in **Table 3** and compared it with the other studied protocols. The average message loss ratio is defined as the average ratio between the number of messages dropped every 300 ms due to cryptographic delays and the total number of messages received in every 300 ms. This can be calculated from the maximum number of signatures and certificates that can be verified by a protocol in 300 ms. The ECDSA, BLS, GSIS and our protocol verify a maximum of 125, 17, 10 and 234 messages respectively. **Figure 4** shows the average message loss ratio between the compared schemes with our protocol. We observe that our protocol has the lowest message loss ratio when compared to the other schemes. Since we deploy the batch verification and avoided the certificate verification, our protocol is able to verify more messages than the other compared counterparts.

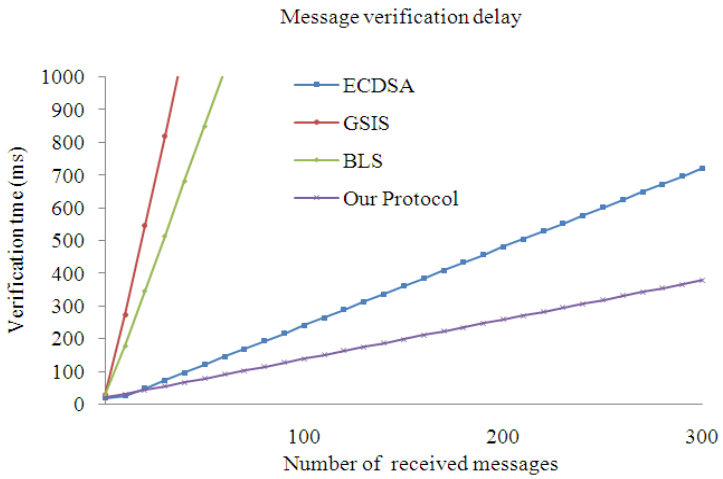

Fig. 2. Message verification delay of compared schemes

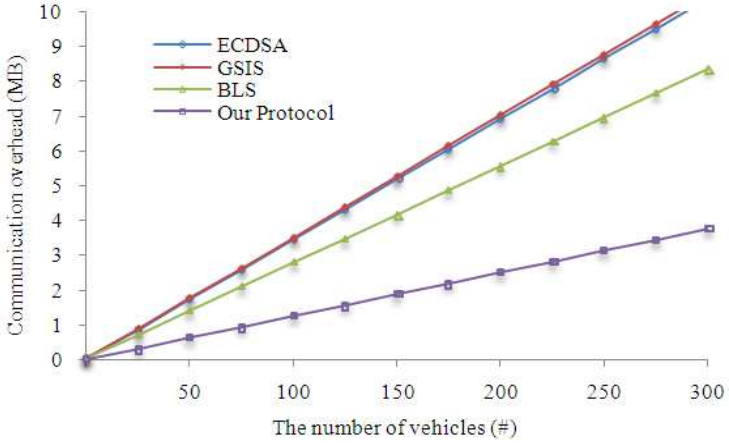

Fig. 3. Communication overhead off compared schemes

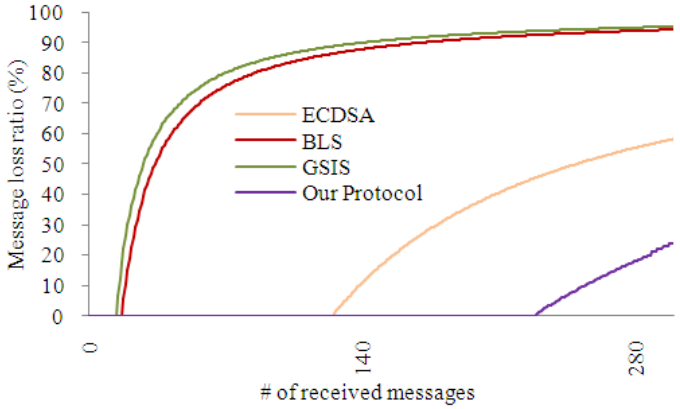

Fig. 4. Message loss ratio of compared schemes

Table 3. NS-2 Simulation Parameters

Description	Values
Simulationarea	7.5×7.5 Km
Simulation time	30000 ms
Maximum speed of vehicles	60 Km/h
OBU transmission range	300 m
MAC protocol	802.11a
OBU data dissemination interval	300 ms
Wired channel capacity	100 Mbps
Wireless channel capacity	6 Mbps
Distribution of RSUs	Uniform

6. CONCLUSION

In this study, we propose a novel RSU based on-the-fly anonymous short-lived public key generation. With our protocol, RSUs are responsible to provide a pseudo-identity to the OBUs, which come into its proximity. The OBUs can generate on-the-fly short-lived public keys using the pseudo-id. This protocol considerably reduces the verification overhead, as it does not require any public key certificate for the authentication of the short-live public keys. This is because; the RSUs periodically publish the valid pseudo-id hashes, which would be used by the vehicles to compare the pseudo-id hashes of the received messages for its trustworthiness. Extensive simulation has been conducted to demonstrate the low overhead and high performance our protocol.

For future research, we will contribute to reduce the signature verification cost for vehicle-to-vehicle communication when the fixed infrastructure such as RSUs is absent in the network.

7. REFERENCES

Boneh, D. and M. Franklin, 2001. Identity-based encryption from the Weil pairing. Proceedings of the 21st Annual International Cryptology Conference, Aug. 1-23, Springer Berlin Heidelberg, Santa Barbara, California, USA., pp: 213-229. DOI: 10.1007/3-540-44647-8_13

Boneh, D., B. Lynn and H. Shacham, 2001. Short signatures from the weil pairing. Adv. Cryptol., 2248: 514-532. DOI: 10.1007/3-540-45682-1_30

Boneh, D., C. Gentry, B. Lynn and H. Shacham, 2003. Aggregate and verifiably encrypted signatures from bilinear maps. Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques, May 4-8, Springer-Verlag Berlin, Poland, pp: 416-432. DOI: 10.1007/3-540-39200-9_26

Calandriello, G., P. Papadimitratos, J.P. Hubaux and A. Lioy, 2007. Efficient and robust pseudonymous authentication in VANET. Proceedings of the fourth ACM International Workshop on Vehicular Ad hoc Networks, Sept. 9-14, New York, pp: 19-28. DOI: DOI: 10.1145/1287748.1287752

Chaum, D. and E. VenHeyst, 1991. Group Signatures. Adv. Cryptol., 547: 257-265.

Choi, H.K., I.H. Kim and J.C. Yoo, 2011. Secure and efficient protocol for vehicular ad hoc network with privacy preservation. EURASIP J. Wireless Commun. Netw. DOI: 10.1155/2011/716794

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

Eastlake, D. and P. Jones, 2001. US Secure hash algorithm 1 (SHA1). ACM Press, United States.

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472. DOI: 10.1109/TIT.1985.1057074

Lin, X., X. Sun, P.H. Ho and X. Shen, 2007. GSIS: A secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol., 56: 3442-3456. DOI: 10.1109/TVT.2007.906878

Lin, X., X. Sun, X. Wang, C. Zhang and P.H. Ho *et al*., 2008. TSVC: Timed efficient and secure vehicular communications with privacy preserving. IEEE Trans. Wireless Commun., 7: 4987-4998. DOI: 10.1109/T-WC.2008.070773

Lu, R., X. Lin, H. Zhu, P.H. Ho and X. Shen, 2008. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. Proceedings of the IEEE 27th Conference on Computer Communications, Apr. 13-18, IEEE Xplore Press, Phoenix, AZ., pp: 1229-1237. DOI: 10.1109/INFOCOM.2008.179

Mak, T.K., K.P. Laberteaux and R. Sengupta, 2005. A multi-channel VANET providing concurrent safety and commercial services. Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, Sept. 02-02, ACM Press, New York, USA., pp: 1-9. DOI: 10.1145/1080754.1080756

Miyaji, A., M. Nakabayashi and S. Takano, 2001. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals Electr. Commun. Comput. Sci., E84-A: 1234-1243.

Raya, M. and J.P. Hubaux, 2005. The security of vehicular ad hoc networks, Proceedings of the 3rd ACM Workshop on SECURITY of Ad Hoc and Sensor Networks, Nov. 07-10, ACM Press, New York, USA., Alexandria, pp: 11-21. DOI: 10.1145/1102219.1102223

Raya, M. and J.P. Hubaux, 2007. Securing vehicular ad hoc networks. J. Comput. Sec., 15: 36-68.

Ren, K., W. Lou, K. Kim and R. Deng, 2006. A novel privacy preserving authentication and access control scheme for pervasive computing environments. IEEE Trans. Vehicular Techonol., 55: 1373-1384. DOI: 10.1109/TVT.2006.877704

Scott, M., 2007. Efficient implementation of cryptographic pairings.

Sha, K., Y. Xi, W. Shi, L. Schewiebert and T. Zhang, 2006. Adaptive privacy-preserving authentication in vehicular networks. Proceedings of the First International Conference on Communications and Networking in China, Oct. 25-27, IEEE Xplore Press, Beijing, pp: 1-8. DOI: 10.1109/CHINACOM.2006.344746

Sweeney, L., 2002. K-Anonymity: A model for protecting privacy. Int. Jo. Unc. Fuzz. Knowl. Based Syst., 10: 557-570. DOI: 10.1142/S0218488502001648

USDT, 2006. National highway traffic safety admin. Vehicle Safety Communications Project, Final Report.

Xi, Y., K. Sha, W. Shi, L. Schewiebert and T. Zhang, 2007. Enforcing privacy using symmetric random key-set in vehicular networks. Proceedings of the 8th International Symposium on Autonomous Decentralized Systems, Mar. 21-23, IEEE Xplore Press, Sedona, AZ., pp: 344-351. DOI: 10.1109/ISADS.2007.37

Xi, Y., W. Shi and L. Schewiebert, 2008. Mobile anonymity of dynamic groups in vehicular networks. Sec. Commun. Netw., 1: 219-231. DOI: 10.1002/sec.28

Xiong, H., K. Beznosov, Z. Qin and M. Ripeanu, 2010. Efficient and Spontaneous privacy-preserving protocol for secure vehicular communication. Proceedings of the IEEE International Conference on Communications, May 23-27, Cape, pp: 1-6. DOI: 10.1109/ICC.2010.5502673

Xu, Q., T. Mak, J. Ko and R. Sengupta, 2007. Medium access control protocol design for vehicle-vehicle safety messages. IEEE Trans. Vehicular Technol., 56: 499-518. DOI: 10.1109/TVT.2007.891482

Zhang, C., R. Lu, X. Lin, P.H. Ho and X. Shen, 2008b. An efficient identity-based batch verification scheme for vehicular sensor networks. Proceedings of the IEEE 27th Conference on Computer Communications, Apr. 13-18, IEEE Xplore Press, Phoenix, AZ., pp: 246-250. DOI: 10.1109/INFOCOM.2008.58

Zhang, C., X. Lin, R. Lu and P.H. Ho, 2008a. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. Proceedings of the IEEE International Conference on Communications, May 19-23, IEEE Xplore Press, Beijing, pp: 1451-1457. DOI: 10.1109/ICC.2008.281