A Secure RSU-Aided Aggregation and Batch-Verification Scheme for Vehicular Networks

Sagarika Mohanty, Debasish Jena and Saroj Kumar Panigrahy

Abstract – In Vehicular adhoc networks, due to the limited bandwidth, high vehicle mobility and density of vehicles, scalability is a major problem. Data aggregation is a solution to this. The goal is to combine the information and disseminate this in larger regions. Another criteria is all the messages should be unaltered in the delivery and should be authenticated i. e. authentication and integrity of the messages should be verified. In this paper, a certificateless aggregate signature protocol for vehicular networks has been proposed which makes RSU responsible for authentication, aggregation and verification of messages sent from vehicles. The RSU is also responsible for notifying the results back to the vehicles within its communication range, to other neighboring RSUs and to the application server for further analysis. Here,we adopt batch verification technique such that verification time can be reduced. The proposed scheme is based on bilinear pairing and hard computational elliptic curve discrete logarithmic problems(ECDLP). The scheme achieves conditional privacy preservation due to the use of pseudo-identity, while a Trust authority(TA) can always retrive the real identity.

Keywords – Aggregation, Dissemination, Privacy, Security, Vehicular adhoc networks

I. Introduction

DUE to the advances and wide deployment of wireless communication technologies in motorized vehicles, many research challenges are opened up in the area of vehicular adhoc networks (VANETS). By being equipped with sensing, processing and wireless communication devices, Vehicles can communicate with each other(V2V communications) as well as with fixed roadside units(V2I communications) located at fixed points in order to provide information about road safety,traffic management and infotainment information to its drivers and passengers.

Security is one of the most significant challenge in the deployment of VANETS. Although academic and industrial research efforts are going on still many open research challenges are there. In a network with high node mobility, strong message authentication with integrity is the primary requirement. Another requirement of VANETs is to protect the privacy of participating nodes and user related information.

According to Dedicated Short-Range Communication (DSRC) protocol [1], a vehicle sends each message within a time interval of 100–300 ms. In a high density traffic scenario, verifying a large number of signatures will put a high computation burden on the receiver. So, the security overhead is more than the message content. Thats why the use of data aggregation.

To address the above issues, in this paper, we propose a RSU-aided aggregation, authentication and batch-verification scheme. The remainder of the paper is organized as follows. Related work is discussed in Section II. In Section III, preliminaries related to the proposed protocol along with the network model, security requirements and pairing concepts are explained. In Section IV, our proposed protocol is explained in detail. In Section V, security analysis and performance evaluation are presented followed by concluding remarks in section VI.

Sagarika Mohanty was with International Institute of Information Technology Bhubaneswar, Odisha, India. (e-mail: sagarikam_23@yahoo. com)

Debasish Jena is with International Institute of Information Technology Bhubaneswar, Odisha, India (corresponding author to provide phone:+91-674-3016019; e-mail: debasish@iiit-bh. ac. in).

Saroj Kumar Panigrahy is with National Institute of Technology Rourkela, Odisha, India. (e-mail: skp.nitrkl@gmail.com)

II. Related Work

Security and privacy issues in VANETs have been studied by many researchers like J. P. Hubaux et al. [2] and Raya et al. [3] which uses PKI(Public Key Infrastructures) based scheme. Compared to the efforts given to security and privacy issues very little attentions have been given to data aggregation in VANETs. Picconi et al. [4] classified aggregation technique as *syntactic* and *semantic*. The main focus of Raya et al. [5] is message aggregation and group communication. They proposed three types of combined signature techniques. Zhang et al. [6] introduced a RSU-aided message authentication scheme(RAISE),where RSU is responbsible for verifying the authenticity of each message. Zhang et al. [7] introduced a identity-based batch signature verification scheme in which an RSU can verify multiple received signatures such that the total verification time can be significantly reduced. Zhu et al. [8] and Wasef et al. [9] propose aggregate signature technique. Tseng et al. [10] propose a secure aggregated message authentication (SAMA) scheme in certificateless public key settings to validate emergency messages in VANETS. In their scheme, the vehicle makes use of the partial private key generated by the KGC and the private key chosen by it to generate the signatures on the emergency messages. In their inter-vehicle communication, aggregation and batch verification is done by the vehicle. Our proposed scheme extends Tseng et al. scheme. In Tseng et al. scheme the communication is V2V, whereas in our scheme communication is between vehicle to roadside (V2I).

III. Preliminaries

A. *Network Model*

Fig. 1 shows a two-layer vehicular network model in which the lower layer includes vehicles and RSUs and communication among them is based on 5. 9 GHz DSRC protocol identified as IEEE 802. 11p. The upper layer is composed of TA and the application server. The RSUs are connected with each other through secure channels, such as the transport layer security (TLS) protocol, with either wired or wireless connection. Similarly, RSUs communicate with the TA and application server through TLS protocol.

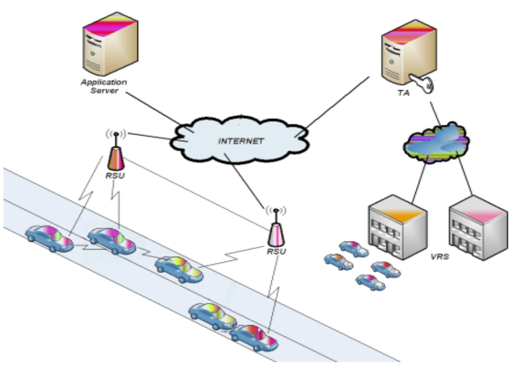

Fig. 1 The Network Model

B. *Security Requirements*

Message Authentication and Message Integrity: Messages from vehicles have to be authenticated to confirm that they are sent unaltered.

Conditional Privacy Preservation: Identities of vehicles should be hidden from a message receiver to protect the senders' private information like vehicle's position, driver's identity etc. Therefore, pseudo-identities are used in place of real identity to protect it.

Identity Traceability: TA should have the ability to retrieve a vehicle's real identity from its pseudo-identity when the message is bogus or there is a dispute.

IV. Proposed Protocol

In this section, we propose a secure RSU-aided aggregation and message authetication with batch verification scheme for transmission of emergency messages. Our proposed protocol is based on *bilinear pairing* and hard computational *Elliptic Curve Discrete Logarithm Problem (ECDLP)*[11]. The bilinear map $\hat{e}$ can be constructed using the modified Weil [12] and Tate pairing [13] on the elliptic curves.

A. *System Setup*

TA sets up the following basic parameters as follows:

Let G be a cyclic additive group generated by P with a prime order q, and G_T be a cyclic multiplicative group of the same order. Let $e: G \times G = G_T$ be a bilinear map. We consider G is represented by 161 bits and the prime order q is represented by 160 bits.

TA first chooses random numbers $m1, m2 \in Z_q^*$ as its two master keys and sets $T_{pb1} = m1P$ and $T_{pb2} = m2P$ as its public keys respectively.

B. Registration: *TA is responsible for registration of $RSUs$ and $OBUs$ [14].*

Algorithm 1: Registration Algorithm

Data: System parameters: $\{G, G_T, e, q, P, H_1, H_2, H_3\}$; RSU identity, location information and public key or OBU identity information.

Output: RSU or OBU register at the TA and obtain the certificate or pseudo-id and partial private key respectively.

Begin

if an RSU needs to register then

get the location information L_k ,its id ID_k and public key Pbr_k from RSU , R_k ;

compute $H_1(ID_k \| L_k \| Pbr_k)$ and store it in Q_k ;

calculate certificate $Cert_k = m1Q_k$;

return $Cert_k$;

else if an OBU needs to register then

get the identity information VID_j and public key Pbv_j ;

calculate the pseudo-id $PID_j = E_{m2}(T_{pb2} \oplus VID_j)$;

compute the partial private key $Ppv_j = m2Q_j$

where $Q_j = H_1(PID_j \| T, Pbv_j)$;

store (PID_j, VID_j) ;

return (PID_j, Ppv_j);

End

Correctness of the certificate can be checked by,

$$e(Cert_k, P) = e(Q_k, T_{pb1}) .$$

C. *Message Signing*

To ensure the integrity of the message each message sent by a vehicle should be signed before being transmitted. When an emergency event EV_i is sensed by the vehicle V_j observation by OBU is $(TID_i, L_{evi}, T_{evi})$, where TID_i is the identity of the type of emergency event i, L_{evi} is the location of event i and T_{evi} is the event time. Vehicle V_j also stores its speed and position information.

Step 1: V_j computes a pair $(M_j^{\ i}, U_j)$ as follows:

$$M_j^{\ i} = H_2(TID_i \,\|\, L_{ev^i} \,\|\, T_{evi})$$

$$U_j = H_3(TID_i \,\|\, L_{evi} \,\|\, T_{evi} \,\|\, Spd_j \,\|\, Pos_j \,\|\, TS_{vj} \,\|\, PID_j \,\|\, Pbv_j)$$

Step 2: With the private key (x_j, Ppv_j), V_j generates the signature as: $\sigma_j^{\ i} = Ppv_j U_j + x_j M_j^{\ i}$

Now, the vehicle V_j contains the emergency event information packet as

$$EV_i = (TID_i, L_{evi}, T_{evi}, Spd_j, Pos_j, TS_{vj}, PID_j, \sigma_j^{\ i}, Pbv_j)$$

TRANSMISSION

Vehicle V_j sends the packet to its nearest RSU by encrypting the packet with the public key of RSU. When the packet reaches RSU it will decrypt it using its private key. According to DSRC [1] the transmission of safety message takes place every 100-300 ms.

D. Aggregated Authentication

RSU is responsible for aggregating multiple authenticated messages in a single packet. Here, we have used *syntactic aggregation of messages* and *cryptographic aggregation of signatures*. The detailed process are given as follows:

Step 1: R_k checks PID_j and verify $(T - TS_{vj}) \le \Delta t$, where T is the current timestamp when receiving the message, TS_{vj} is the timestamp when sending the message and Δt denotes the expected time interval for the transmission delay.

Step 2: If this holds true, then R_k process the packet and aggregate it according to its emergency type-id (TID). The packets with higher emergency level will be processed first.

Step 3: Then it computes the average speed.

Step 4: TID, L_{ev} and T_{ev} are same for all.

Step 5: Signature aggregation: Then the aggregator R_k computes the aggregate signature σ_{agg} as follows:

$$\sigma_{agg} = \sum_{j=1}^{n} \sigma_j^{\ i} = \sum_{j=1}^{n} (Ppv_j U_j + x_j M_j^{\ i})$$

Step 6: After aggregation, the aggregator R_k get the aggregated emergency report ER_{agg} as follows:

$$\mathrm{ER_{agg}} = (\mathrm{PID_1}, \mathrm{PID_2}, \ldots \mathrm{PID_n}, \mathrm{TID}, \mathrm{L_{ev}}, \mathrm{T_{ev}}, \mathrm{Spd_{avg}}, \mathrm{Pos_{v1}}, \mathrm{Pos_{v2}}, \ldots, \mathrm{Pos_{vn}}, \mathrm{TS_{v1}}, \mathrm{TS_{v2}}, \ldots, \mathrm{TS_{vn}}, \sigma_{\mathrm{agg}}, \mathrm{Pbv_1}, \mathrm{Pbv_2}, \ldots \mathrm{Pbv_n})$$

BATCH VERIFICATION

RSU verify the signature of the message to ensure that the corresponding vehicle is not attempting to impersonate any other authorized vehicle or disseminating bogus messages. Fisrt, we have presented single signature verification followed by batch signature verification.

Single signature verification: The signature is valid if,

$$e(\sigma_j^{\ i}, P) = e(Q_j U_j, T_{pb2}) e(M_j^{\ i}, Pbv_j).$$

Batch Verification: The signature is valid if,

$$e(\sigma_{agg}, P) = e(\sum_{j=1}^{n} Q_j U_j, T_{pb2}) e(M^i, \sum_{j=1}^{n} Pbv_j)$$

This batch verification can significantly reduce the verification delay when verifying a large number of signatures. After verification the aggregated packet will be disseminated to all vehicles within the communication range of the RSU, to its neighboring $RSUs$ to disseminate the information in larger regions and to the application server for further analysis.

E. Message Transmission to Neighboring RSUs

$RSUs$ need to authenticate themselves to TA periodically. If the TA finds a compromised RSU, it will immediately inform its neighbors about that compromised RSU [15]. The aggregator RSU sends the emergency information to its neighboring $RSUs$ to disseminate it in larger areas. The packet contains the following information:

$$ER = (RID_k, Loc_{Rk}, TID, L_{ev}, T_{ev}, Spd_{avg}, Pos_{v1}, Pos_{v2}, \ldots, Pos_{vn}, TS_{Rk}, Cert_k)$$

The packet will be encrypted by the private key of the sender RSU. When it reaches the neighboring RSU it will decrypt it using the sender RSU's public key and do the following steps:

Step 1: Check RID_k, Loc_{Rk} and verify $(T - TS_{Rk}) \le \Delta t$, where T is the current timestamp when receiving the message by the neighboring RSU, TS_{Rk} is the timestamp when sending the message by the sender RSU and Δt denotes the expected time interval for the transmission delay.

Step 2: If found valid, then verify the certificate.

Step 3: If verification result is satsfied, then accept the message and disseminate this within its own range.

Step 4: If not valid, reject the message.

V. Security Analysis And Performance Evaluation

A. Security Analysis

Resilience to Replay attack: The receiving RSU will check if the time information is within the allowable time frame. The verification fails if $(T' - TS_{vj}) > \Delta t$, where T' is the system time when receiving the replayed message. Similarly,while transmitting to neighboring $RSUs$, the receiving RSU check if $(T' - TS_{Rk}) > \Delta t$,then reject the message.

Resilience to Forgery attack: Due to the use of hard ECDLP problem, the proposed protocol is unforgeable. Having no idea about the partial private key Ppv_j and a secret key x_j, an attacker cannot compute a valid signature and hence cannot launch a forgery attack. It is computationally infeasible to find out x_j from Pbv_j because of the use of ECDLP.

Conditional Privacy Preservation: In the proposed scheme, without knowing the master-key $m2$ and T_{pb2} ,it is not possible for anyone to find out the real identity from its pseudo-identity.

Identity Traceability: Given the pseudo-identity PID_j, only TA with its master key $m2$ and T_{pb2} ,can trace the real identity as follows:

$$D_{m2}(PID_j) = D_{m2}(E_{m2}(T_{pb2} \oplus VID_j) = VID_j$$

Resilience to RSU Replication Attack: When a neighboring RSU receives the emergency message, the receiving RSU will compare the physical location of the sender RSU with the location information specified in the packet. The RSU will discard the message if the location information verified is different.

B. *Performance Evaluation*

Here, we evaluate the performance of the proposed scheme in terms of verification delay. In the verification phase, we neglect the operations such as additive and one-way hash function since they are insignificant to the computational cost. Multiplication in Z_q^* are ignored since they are much smaller than other operations [16].

TABLE 1. FIVE SIGNATURE SCHEMES IN TERMS OF VERIFYING A SINGLE SIGNATURE AND N SIGNATURES RESPECTIVELY.

	Verify a single signature	verify n signatures
$ECDSA$	$4T_{mul}$	$4nT_{mul}$
BLS	$4T_{pair} + 2T_{mtp}$	$(2n+2)T_{pair} + 2nT_{mtp}$
CAS	$5T_{pair} + 2T_{mtp}$	$(4n+1)T_{pair} + 2nT_{mtp}$
$ASIC$	$5T_{pair} + 3T_{mul}$	$5T_{pair} + 3nT_{mul}$
Proposed	$3T_{pair} + 1T_{mul}$	$3T_{pair} + nT_{mul}$

Let T_{pair} denote the time required to perform a bilinear pairing operation, T_{mul} denote the time to perform one point multiplication over an elliptic curve and T_{mtp} denote the time of a MapToPoint hash operation. In [13], T_{pair} , T_{mtp} , T_{mul} are found for a supersingular curve with embedding degree k=6 to be equal to 4. 5 msec,3. 9 msec and 0. 6 msec respectively.

It can be easily known that pairing operations are the time consuming operations compared to other operations [13],[17]. Fig. 2 shows the verification delay in miliseconds vs. traffic density. It can be seen that the proposed protocol provides the lowest verification delay among the protocols under consideration.

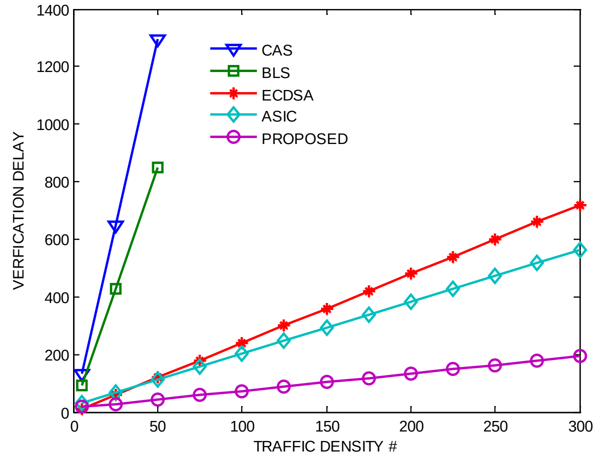

Fig. 2 Verification delay vs. Traffic density

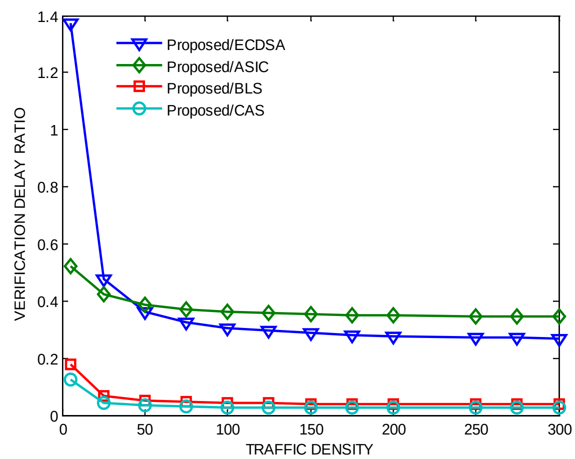

Fig. 3 Verification delay ratio vs. Traffic density

In Fig. 3 we compare the message verification dalay of these five schemes in terms of the ratio of the verification delay. We can see that the delay ratio between Proposed and ECDSA[18] approaches to a constant, which is approximately 0. 2781, for ASIC[9] it is 0. 349 and for BLS[19] it is 0. 388 when the number of messages in one interval is nearing 200. The delay ratio between Proposed and CAS[20] is approximately 0. 0284 when the number of messages is nearing 75. In other words, the speed of Proposed scheme is 72% faster than that of ECDSA, 65% faster than that of ASIC, 96% faster than that of BLS and 97% faster than that of CAS. The length of an emergency message format in the proposed protocol is shown in Table 2. Since q is a 160-bit prime and each element in G is 161 bits long, we get the size of the signature as 40 bytes. Therefore, the communication overhead incurred in broadcasting an emergency packet from the vehicle to the RSU is 95 .

TABLE 2. EMERGENCY MESSAGE FORMAT (IN BYTES)

TID_i	L_{evi}	T_{evi}	Spd_j	Pos_j	TS_{vj}	PID_j	σ_j^i	Pbv_j
2	8	4	1	8	4	8	40	20

VI. Conclusion

The main idea of our proposed scheme is to disseminate the emergency message to larger regions so that secondary accidents can be avoided. In this, it achieves security and conditional privacy preservation by using pseudo-identities, though TA can always trace the real identity if any dispute happens. The scheme reduces the bandwidth and achieves scalability by aggregating the signature. The verification time is reduced due to batch verification technique. In addition, our scheme can prevent forgery attacks and all possible reply attacks. The merits of our proposed scheme are analysed through security analysis and performance evaluation. In our future work, we will continue our efforts to address other security issues in vehicular adhoc netwoks, such as Denial of Service (DoS) attack and other aspects of dissemination.

References

[1] Dedicated Short Range Communications (DSRC). [Online] Available: http://grouper. ieee. orglgroups/scc32/dsrc/index. html

[2] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, 2004.

[3] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, vol. 15, no. 1, 2007, pp. 39- 68.

[4] Picconi F, Ravi N, Gruteser M, Iftode L, "Probabilistic validation of aggregated data in vehicular ad-hoc networks. In: VANET '06: Proceedings of the 3rd international workshop on vehicular ad hoc networks. New York, NY, USA: ACM; 2006. pp. 76–85.

[5] Raya M, Aziz A, Hubaux J. P. "Efficient secure aggregation in vanets", In VANET '06, Proceedings of the 3rd international workshop on vehicular ad hoc networks New York, NY, USA, ACM; 2006. pp. 67–75.

[6] C. Zhang, X. Lin, R. Lu, P. -H. Ho and X. Shen,"An Efficient Message Authentication scheme for Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 57, No. 6, Nov. 2008.

[7] C. Zhang,R. Lu, X. Lin, P. -H. Ho and X. Shen, "An Efficient Identity based Batch Verification scheme for Vehicular Sensor Networks", in Proc. IEEE INFOCOM, 2008, pp. 246 - 250, Phoenix, AZ, April 2008.

[8] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks" in Proc. IEEE ICC, 2008 ,pp. 1436-1440.

[9] Albert Wasef, Xuemin (Sherman) Shen,"ASIC:Aggregate signature and Certificate Verification Scheme for Vehicular Networks", Available at: http://www. engine. lib. uwaterloo. ca.

[10] Huei-Ru Tseng, Rong-Hong Jan, Wuu Yang, Emery Jou, "A Secure Aggregated message authentication scheme for Vehicular Ad-Hoc Networks", 18th World congress on Intelligent Transportation systems, 2011.

[11] N. Koblitz,A. Menezes,S. Vanstone, "The state of elliptic curve cryptography", Design,Codes and Cryptography, vol. 19, No. 2, pp. 173-193,Mar. 2000.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in Proc. Crypto, LNCS,vol. 2139, pp. 213-229, 2001.

[13] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Transactions on Fundamentals,Vol. E84-A, No. 5, pp. 1234-1243, 2001.

[14] D. R. Stinson, Cryptography: Theory and practice. Boca Raton, FL,Chapman &Hall/CRC, 2006.

[15] Xiaoping Xue and Jia Ding,"LPA: a new location-based privacy-preserving authentication protocol in VANET", Security and Communication Networks, 2011,vol. 5,pp. 69-78.

[16] "Crypto++ 5. 6. 0 Benchmarks", http://www. cryptopp. com/benchmarks. html.

[17] M. Scott, "Efficient implementation of crytographic pairings," [Online]. Available: http://ecrypt-ss07. rhul. ac. uk/ Slides/Thursday/mscott-samos07. pdf.

[18] IEEE Standard 1609. 2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, 2006.

[19] D. Boneh, C. Gentry, B. Lynn, H. Shacham,"Aggregate and Verifiably Encrypted Signatures from Blinear Maps", Advances in Cryptology-EUROCRYPT 2003,LNCS 2656, pp. 416-432,2003.

[20] Zheng Gong, Yu Long, Xuan Hong, Kefei Chen," Two Certificateless Aggregate Signatures from Bilinear Maps", SNPD 2007, IEEE Computer Society Proceedings, pp. 188-193. August 2007.