RESEARCH PAPER | Computer Science | Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

An Efficient Authentication Scheme for Vanet Using Cha Cheon's ID Based Signatures

KEYWORDS: Authentication, Signature generation, Signature verification, VANET, Cha Cheon's ID based signature

Y.Bevish Jinila
Research Scholar, Faculty of Computing, Sathyabama University,Chennai, India

K. Komathy
Professor, Easwari Engineering College,Chennai, India

ABSTRACT *Authentication of safety messages in Vehicular Ad hoc Networks (VANET) plays a major role. The time take for signature generation and verification should be very less, to provide a secure and comfortable transportation to the public. Several signature generation and verification schemes are proposed in the literatures. This paper focusses on the usage of Cha Cheon's ID based signature scheme for authentication in vehicular networks. Experimental analysis shows that this signature scheme incurs less signature size, less delay and less overhead in transmission when compared to the existing schemes.*

1. INTRODUCTION

The Vehicular Ad hoc Network (VANET) is an emerging intelligent network which offers safety and comfort to the public on travel. The primary purpose of a vehicular network is to enable communication for automotive safety applications. This network includes a centralized Trusted Authority (TA) responsible for the registration of the vehicle in the network and maintaining the information relevant to the registered users. It involves several Road Side Units (RSUs) deployed on road sides separated by certain miles. These RSUs are responsible for communicating the safety information with the vehicles travelling in its range. In addition, it is responsible for verifying the authenticity of the users reporting the occurrence of the events in its communication range. Each vehicle is equipped with an On Board Unit (OBU) which enables vehicle to communicate with each other.

The safety messages are broadcasted for every 100 to 300 milliseconds. The received messages are verified for authenticity of the sender's identity. However, a vehicular network is a very high speed network where even a small delay can cause serious issues. Hence the process of authentication should be done in a very short time. Several literatures have used different types of signature generation and verification methods to improve the authenticity in vehicular networks. It is required to analyze the best signature scheme which can be applied to such networks to make the process of authentication easier and efficient. In this paper, recent three signature schemes namely the public key signature scheme ECDSA, CPAS and the Cha Cheon's ID based signature scheme is compared and analyzed.

The rest of the paper is organized as follows. Section 2 focusses on the Cha Cheon's ID based signature scheme. Section 3 discusses the related work. Section 4 analyses the signature schemes and Section 5 concludes the work and proposes future directions for extension.

2. CHA CHEON'S SIGNATURE SCHEME

This section focusses on the Cha Cheon's ID based signature scheme used in the proposed approach.

Cha Cheon is an ID based signature scheme which consists of four algorithms namely setup, extract, sign and verify. Figure 1 show the general structure of the ID based signature scheme where the sender ID is used as the public key for verification. The notations used in this paper are listed in Table 1.

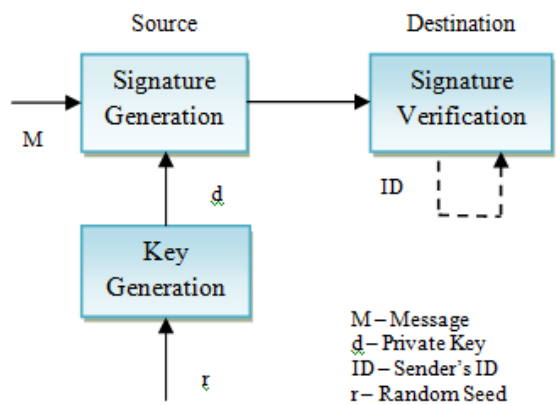

Figure 1: ID based Signature Scheme

Setup

The Private Key Generator (PKG) chooses 's' as the master secret key and computes the public key as shown in equation (1).

$$P_{pub} = sP \quad (1)$$

In addition, it chooses a map to point hash function H1 : {0,1} $\rightarrow G_1$ and another cryptographic hash function H2 : {0,1}* * $G_1 \rightarrow Z/q$.

Extract

The PKG verifies the given ID and computes the secret key for the given ID as shown in equation (2). Then, the public key is computed as shown in equation (3).

$$S_{ID} = s\, H_1(ID) \quad (2)$$

$$Q_{ID} = H_1(ID) \quad (3)$$

Sign

To sign a message m $\in$ {0,1}* using the private key S_{ID}, the signer chooses choose an integer r $\in Z/q$ and computes the equations (4),(5) and (6). The signature, σ = <U,V> $\in G_1 * G_1$

$$U = r\, Q_{ID} \quad (4)$$

$$h = H_2(m, U) \quad (5)$$

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

$V = (r + h)\, S_{ID}$ (6)

Verify

To verify a signature $\sigma = <U,V>$ of an identity ID on a message 'm' equation (7) is used.

$e(P,V) = e(P_{pub}, U + hQ_{ID})$ (7)

TABLE – 1
NOTATIONS USED

Notation	Description
TA	Trusted Authority
RSU	Road Side Unit
G	A cyclic additive group
P	The generator of the cyclic additive group G
q	The prime order of group G
r	Random seed
P_{ID}	Pseudo Identity of the vehicle
PKG	Private Key Generator
e	Mapping Function
H ( )	Hashing Function SHA-1

3. RELATED WORK

Safety messages send from the vehicles to the RSU has to be verified for the authenticity of the sender before it is considered to be reliable. Else, an adversary can misuse the medium to transfer fake messages thereby degrading the performance of the network. Before the vehicular network is deployed for enabling the safety applications, the security issues should be resolved. Recently, several works have been proposed addressing the security issue namely the authentication in VANET. Raya et. al. [1] proposed a security scheme for message authentication using conventional public key cryptography.

The IEEE 1609.2 [2] has proposed the use of ECDSA (Elliptic Curve Digital Signature Algorithm) for vehicular network authentications. This is a public key approach of digital signatures. Using, ECDSA incurs more processing delay at the receiver's side. Though the delay may be in order of certain milliseconds, there may be a possibility for the messages being discarded during heavy traffic conditions. Sensitive safety messages when discarded causes a great havoc in vehicular network.

The authors in [3] have proposed a protocol ABAKA which is based on the elliptic curve cryptography for authentication. They have also proposed the pseudo identities for privacy preservation. The authors have compared their results with ECDSA and it is shown that ABAKA has less signature size and less verification time when compared to ECDSA. But, this scheme is suitable for value added services and the authors have not mentioned the use of their protocol for safety message communication. The authors in [5],[6],[7] proposed the use of public key signatures for generation and verification in vehicular networks.

Lin et. Al. [8] proposed a group signature based technique which provides conditional privacy without pseudonym change. This is a centralized group signature protocol which also combines the features of id based signatures. Lei et. al. [11] proposed a privacy preserving authentication protocol. The authors have listed the drawbacks of GSIS protocol [9,11,12] and they have proposed a decentralized group signature protocol. The challenges like certificate distribution and revocation, limiting the amount of communication and computational bottleneck. This scheme doesn't strongly depend on any tamper proof device. In this approach, RSUs are used to maintain the on the fly generated group within their communication range. The limitation with this approach is that when a particular RSU fails, the vehicles moving in that area will be heavily affected. If there is an emergency situation to be communicated, a single point of failure can cause a great havoc to the vehicular applications.

Shamir [4] proposed the use of ID based signature scheme to overcome the limitations of public key signature schemes. Zhang et. al [13] proposed an ID based verification scheme (IBV) for vehicular networks based on pairing based cryptography. Compared with the public key signature scheme, the signature size is very less and signature verification is faster. It uses three pairing operations. Since the verification speed of a pairing operation is slower than the multiplication operation this scheme suffers from replay attacks. Jiun Long Huang et. al [14] proposed an authentication scheme which is a modified version of ECDSA. This scheme performs better when compared to the IBV scheme in terms of verification delay, transmission overhead and verification cost. However, this scheme will not be suitable for batch verifications.

An efficient privacy preserving authentication scheme proposed by Kyung shim [15] uses a new ID based signature scheme. This scheme provides less verification delay and signature size when compared to Zhang et. al. approach. The map to point hash function used in Zhang et. al approach is removed in this scheme. This scheme uses three pairing operations and one multiplication operation. The cryptographic cost incurred is less when compared to the IBV scheme and the time for verifying 800 signatures is reduced to 18% when compared to IBV scheme. However, since the verification speed is dependent on the cryptographic computational complexity, the number of pairing operations should be minimal. Since, this scheme uses three pairing operations it is susceptible to a higher verification delay when the number of signatures crosses a particular threshold.

To summarize, all these existing schemes incurs more overhead and verification delay.

4. PERFORMANCE EVALUATION

This section analyses the performance of the proposed signature scheme namely the Cha Cheon's ID based signature with the existing ECDSA and CPAS scheme based on factors like signature verification delay and transmission overhead. The performance of the two signature schemes is tested under Pentium IV, 2GHz, and Windows 7 system on Java platform.

Figure 1 : Login to the System

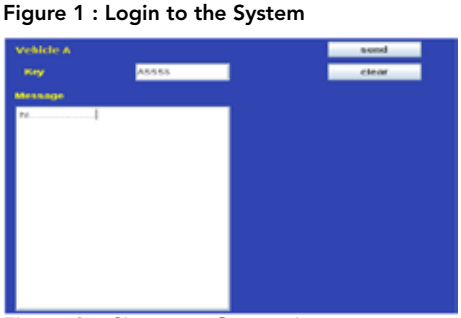

Figure 2 : Signature Generation

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

Figure 3 : Signature Verification

Figure 1 shows the login to the system. Figure 2 shows the signature generation and figure 3 shows the signature verification. The performance was evaluated for 10 to 50 signatures.

4.1 Verification Delay

The time cost of the cryptographic operations required for verification should be computed to calculate the verification delay. Three main cryptographic operations are considered for evaluation. Let T_{mul} represent the time taken for one point multiplication over an elliptic curve, T_{par} represent the time taken for one pairing operation and T_{mtp} represent time taken for a map to point hash function.

The number of cryptographic operations required for verification in ECDSA requires $4T_{ml}$. For verifying 'n' signatures, the cryptographic overhead incurred is $4nT_{ml}$. The cryptographic operations required for verification of CPAS scheme requires $3T_{par} + T_{mtp} + T_{mul}$. For 'n' signatures the time incurred is equal to $3T_{par} + nT_{mtp} + nT_{mul}$. The cryptographic operations incurred for verification in Cha cheon'd ID based signature scheme requires $2T_{par} + T_{mtp} + T_{mul}$. So, for verifying 'n' signatures the time incurred is equal to $2T_{par} + nT_{mtp} + nT_{mul}$.

In this analysis, it is assumed that the RSUs are deployed for each 1 km range. Figure 4 shows the time taken for signature verification for various schemes. The 'x' axis denotes the traffic density which represents the total number of vehicles in the communication range of an RSU and the 'y' axis represents the time in milliseconds.

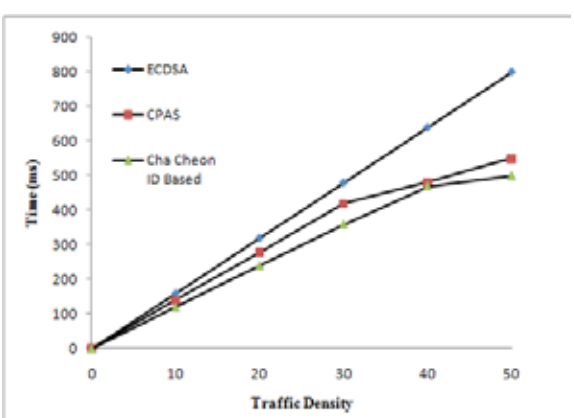

Figure 4: Signature Verification Time

Figure 5 shows the relationship between the total number of vehicles in the communication range of an RSU and the verification delay. From figure 5 it is evident that the proposed scheme incurs less verification delay when compared with ECDSA and CPAS schemes.

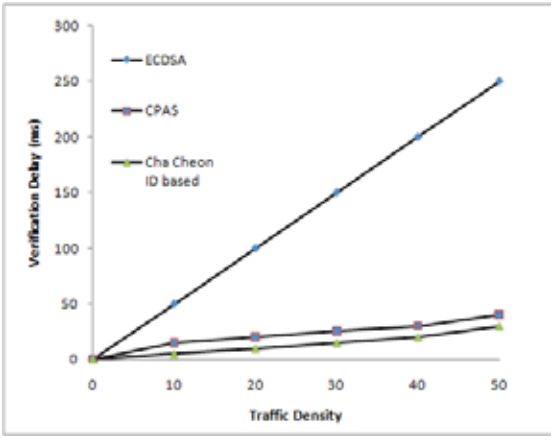

Figure 5: Signature Verification Delay

4.2 Transmission Overhead

In this section, the transmission overhead incurred while sending the messages from the vehicles to the RSU is analyzed. Table 2 shows the transmission overhead of the two schemes. The transmission overhead includes the signature and the certificate and the message is not included.

TABLE – 2
COMPARISON OF TRANSMISSION OVERHEAD

Scheme	Send a Single Message	Send 'n' Messages
ECDSA	42+125 bytes	42n+125n bytes
CPAS	18 + 42 bytes	18 + 42n bytes
Cha Cheon	16+42 bytes	16+42n bytes

Figure 6 shows the relationship between the number of requests received by the RSU and the transmission overhead incurred. From figure 6 it is evident that the transmission overhead for the proposed scheme Cha Cheon's ID based signature scheme incurs less overhead when compared to the existing schemes.

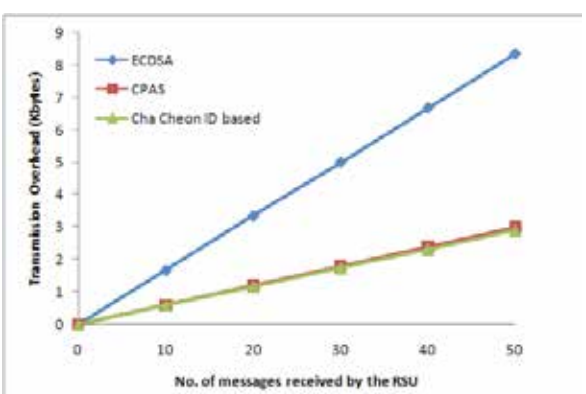

Figure 6: Transmission overhead vs the number of requests

CONCLUSION

This paper has proposed the use of Cha Cheon's ID based signature scheme for authentication in VANET. From experimental analysis it is evident that this scheme incurs less verification delay and less transmission overhead when compared to the existing approaches. In future, this signature scheme will be combined with the pseudo IDs to generate a privacy preserving authentication protocol.

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

REFERENCE

M. Raya and J.P. Hubaux, "Securing Vehicular Ad hoc Networks", Journal of computing and security, Vol. 15, no. 1, pp. 39-68, Jan 2007. | Tim Weil, " Securing Wireless Access in Vehicular Environments", IEEE GLOBECOM 2008. | Jiun Long Huang, Lo Yao and Hung Yu Chien, " ABAKA : An Anonymous Batch Authenticated and Key Agreement Scheme for Value Added Services in Vehicular Ad hoc Networks", IEEE Transactions on Vehicular Technonogy, Vol.60, Issue.1, 2011. | A. Shamir, " Identity based cryptosystems and signature schemes", in Advances in cryptology-crypto, New York : Springer – verlag , 1984, pp. 47-53. | H. Wen, P.H. Ho, G. Gong, A Novel Framework for Message Authentication in Vehicular Communication Networks, Proceedings of the IEEE GLOBECOM '09, 2009, pp. 1–6. | A. Wasef, X. Shen, MAAC: message authentication acceleration protocol for vehicular ad hoc networks, in: Proceedings of the IEEE GLOBECOM '09, 2009, pp. 1–6. | Fuwen Liu, " A Tutorial on Elliptic Curve Cryptography (ECC), Brandenburg Technical University of Cottbus, Computer Networking Group. | X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communication," IEEE Trans. Veh.Technology, volume 56, no. 6, pp. 3442–3456, Nov. 2007. | Calandriello. G, P. Papadimitratos, J.P. Hubaux and A.Lioy, "Efficient and Robust Pseudonymous Authentication in VANET", Proc. 4th ACM Int. Workshop VANRT, Montreal, QC, Canada, pp. 19-28, Sept 2007. | Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue,"PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs", IEEE Transactions on Intelligent Transportation Systems, volume 12, No. 3, September 2011. | Lei Zhang, Qianhong Wu, Agusti Solanas, Josep, " A Scalable Robust Authentication Protocol for Secure Vehicular Communications", IEEE Transactions on Vehicular Technology, volume 59, No. 4, May 2010. | Y. Sun, R.Lu, X. Lin, X.S.Shen and J.Su," An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", IEEE Transactions on Vehicular Technology, volume 59, No. 7, pp. 3589-3603, Sept 2010. | Zhang, Rong Xing Lu, Xiaodong Lin, Pin Han Ho and Xuemin Shen "An Efficient Identity Based Batch Verification Scheme for Vehicular Sensor Networks", IEEE INFOCOM 2008. | Jiun Long Huang, Lo Yao Yeh and Hung Yu Chien, " An Anonymous Batch Authenticated and Key Agreement Scheme for Value Added Services in Vehicular Ad hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 60, No.1, Jan 2011. | Kyung Ah Shim, "An Efficient Conditional Privacy Preserving Authentication Scheme for Vehicular Sensor Networks", IEEE Transactions on Vehicular Technology, Vol. 61, No. 4, May 2012. |