Certificateless Authentication Scheme in VANETs

Reema Sandhu[1] , Mukesh Kumar Rana[2]

[1]Ph.D Research Scholar, Department of Computer science & Applications, NIILM University, Kaithal, Haryana

[2]Assistant Professor, Department of Computer science & Applications, NIILM University, Kaithal, Haryana

ABSTRACT:

VANETs can be seen as an extension of mobile ad-hoc networks where there are not only mobile nodes, named On-Board Units (OBUs), but also static nodes, named Road-Side Units (RSUs). The so-called Intelligent Transportation System (ITS) includes two types of communications: between OBUs and between OBUs, and RSUs [5]. IEEE 802.11p amendment to IEEE 802.11, which adds a vehicular communication system is the basis for both the European standard for ITS, called ITS-G5, and its American counterpart, called Wireless Access in Vehicular Environment (WAVE). The protection of the security of communications is more difficult due to the open broadcasting of wireless communications and the high-speed mobility of vehicles in VANETs. In these networks, any malicious misbehaving user that can inject false information, or modify/replay any previously disseminated message, could be fatal to the others. Therefore, within the family of standards for vehicular communications IEEE 1609 based on the IEEE 802.11p, the standard 1609.2 deals in particular with the issues related to security services for applications and management messages. This standard describes the use of PKIs, CAs and CRLs, and implies that in order to revoke a vehicle, a CRL has to be issued by the CA to the RSUs, who are in charge of sending this information to the OBUs. In this paper the CLS and CLAS schemes are highlighted and what advantage they have over PKI is also specified. The shortcomings in the implementation of various CLS and CLAS schemes is also highlighted and in future what work can be done to improve them are given in the conclusion at the end.

ISBN: 978-81-955611-3-1

KEYWORDS: Certificateless, Aggregate, Elliptic, Cryptography, Asymmetric, RSA, Authentication

1. INTRODUCTION

Authentication is a critical piece in the security of wireless communications where the existence of effective mechanisms for revocation of users is required. On the one hand, it is necessary to optimize the authentication process so that legitimate and honest nodes can make use of all network services. On the other hand, the authentication process must be useful to detect and exclude the malicious nodes, in order to ensure network reliability. A major problem when communication security is based on public-key cryptography is to ensure that any particular public key is authentic and valid. The traditional approach to this problem is through public-key certificates emitted by a Public Key Infrastructure (PKI), in which a Certificate Authority (CA) certifies ownership and validity of public-key certificates. This solution presents many difficulties because the issues associated with certificate management are quite complicated and expensive. The so-called Identity Based Cryptography (IBC), where each user's public key is his/her public Identity (ID), represents a different approach because the need for public key certificates is eliminated. Efficiency is a key feature in revocation when public-key cryptography is used because private keys may become compromised. This problem has been traditionally solved through a centralized approach based on the existence of a Trusted Third Party (TTP), which is usually a CA distributing the so-called Certificate Revocation Lists (CRLs) that can be seen as blacklists of revoked certificates. In particular, the IEEE 1609.2 standard proposes both broadcast authentication and non-repudiation through the use of the Elliptic Curve Digital Signature Algorithm (ECDSA). However, the verification of each signatureusing ECDSA means a high computational cost. On the one hand, according to these standards, each vehicle is assumed to have a pair of keys: a private signing key and a public verification key certified by the CA; and any VANET message must contain: a timestamp with the creation time, the sender's signature, and the sender's public-key certificate. On the other hand, the socalled Dedicated Short-Range Communications (DSRC), devoted specifically designed for automotive use, defines that vehicles regularly exchange with nearby vehicles beacons containing sender information such as location and speed, because the information of these beacons is very useful for many VANET applications, such as cooperative collision warning. Each OBU can get multiple certified key pairs and use different public keys each time certified in order to protect privacy in VANETs. These public keys

ISBN: 978-81-955611-3-1

are linked to pseudonyms that allow preventing location tracking by eavesdroppers. Therefore, once VANETs are implemented in practice on a large scale, their size will grow rapidly due to the increasing number of OBUs and to the use of such multiple pseudonyms. Thus, it is foreseeable that if CRLs are used, they will grow up to become very large and unmanageable. Moreover, this context can bring a phenomenon known as implosion request, consisting of many nodes who synchronously try to download the CRL during its updating, producing a longer latency in the process of validating a certificate due to serious congestion and overload of the network.

2. RELATED WORK

In VANETs, the security and privacy problems have attracted strong interest and research from industry and academia. Recently, lots of CPPA schemes for VANETs have been put forward and roughly classified into three categories: PKI-based schemes, ID-based schemes, and certificateless schemes. To settle the problem of security and some privacy requirements in VANETs, a number of professors and scholars proposed a kind of new scheme called Public Key Infrastructure-based (PKI-based) authentication schemes. In their schemes, they either tried to make vehicles compute more to verify the signatures from other vehicles or assume that there exists a trusted certificate authority to issue and maintain certificates of various vehicles. However, the assumption may be unrealistic because a single node cannot afford the oceans of calculation. In 2004, Hubaux et al. firstly pointed out the security and privacy issues in VANETs and declared that the public key infrastructure (PKI) technology could be used to protect transmitted messages in the vehicles. In 2007, based on anonymous certificates, an anonymous authentication scheme for VANETs was proposed by Raya and Hubaux showed that the proposed scheme can provide message authentication and conditional privacy preservation. In this scheme, each vehicle requires to preload a huge quantity of anonymous public/private key pairs and corresponding public key certificates and then to sign a message using one of the private keys for anonymity in each communication., therefore, a huge storage space is needed to store keys and corresponding certificates in all vehicles, while the certificate authority also needs to store all vehicles' certificates. In 2008, Lu et al. put forward an efficient conditional privacy preservation (ECPP) scheme for VANETs to solve the problem of a large storage space for the vehicles in by employing the

ISBN: 978-81-955611-3-1

temporary anonymous certificates. Based on the hash message authentication code (HMAC) and k-anonymity approach, an efficient RSU-aided message authentication scheme was proposed by Zhang et al.to realize the privacy preserving of the vehicles. In summary, all the PKI-based authentication schemes for VANETs have a bottleneck problem on the storage and management of certificates. Later, a new kind of signature scheme called identity-based signature (IBS) scheme is widely discussed. For example, Liu et al. proposed an IBS scheme which can take the user's identity as the public key, and the private key is generated by the public key generation PKG, which can reduce a single node's burden. However, IBS has inherent problems about key escrow which is generated by user's identity. In Al-Riyami and Paterson's scheme, they firstly introduce the certificateless public key cryptography. In recent years, a lot of researches on CLS and CL-AS schemes with bilinear pairing have been carried on by relevant researchers. In their schemes, key generation center (KGC) uses its master key and the user's identity information to calculate a part of the private key and send it to the user, whereafter the user combines part of the private key and his/her secret value together to generate the user's real private key which can protect the user's privacy and make the system secure. The above scheme uses the bilinear pairing which costs relatively large computation. The elliptic curve cryptography is chosen to use in the CLS and CL-AS because of its high efficiency. In Xie et al.'s scheme, they proposed rigorous security proof that shows the scheme is able to resist various malicious attacks and ensure privacy protection. In the field of health care, Du et al. proposed a CLAS scheme with high efficiency and low latency which can be more suitable to apply to the field of healthcare. In 2018, Cui et al. demonstrated their novel CLS and CL-AS scheme with ECC, which significantly reduces computing time during sign and verification process. Kamil et al. declared that the scheme proposed by Cui et al. is not secured against the signature forgery attack, and they advanced an improved signature scheme for VANETs. They claimed that their proposed scheme can address all the needs of VANETs about security and privacy in a better way.

3. PRELIMINARIES USED IN CERTIFICATELESS AUTHENTICATION SCHEME

Generally, a certificateless signature (CLS) scheme and a certificateless aggregate signature (CL-AS) scheme consist of the following seven algorithms.

(1) Setup: The KGC and TA will execute this probabilistic algorithm, which

ISBN: 978-81-955611-3-1

needs a security parameter λ, then generates a elliptic curve E, public keys PKTA and PKKGC, and master secrets key α, β, respectively, then publishes a number of system parameters which is used for ensuring the system in order.

(2) Partial Private Key Generation: In this algorithm, firstly, the entity Vi transmits a tuple which includes its real identity and partial pseudo identity to TA. Then TA sends a whole pseudo identity to KGC with calculation. Eventually, KGC transmits the partial private key to entity Vi in a secure channel.

(3) Vehicle Key Generation: The entity Vi selects random ρi Z q as its secret key and calculates its public key PKVi .

(4) Individual Sign: This algorithm is used by each entity Vi; after generating a message mi, the entity Vi tries to calculate a set of variables. Then it sends the signature σ to the verified

(5) Individual Verify: This algorithm is executed by the verifier such as RSU. When receiving input including signature σ, pseudo identity PIDi and current time Tcur, the RSU will check the time validity firstly. Then the algorithm will output true if the signature is valid or false otherwise.

(6) Aggregate Sign: In this algorithm, generally the aggregate signature generator is RSU in our system. For an aggregating set V of n entities V1, V2, , Vn, the pseudo identity PIDi of each vehicle Vi as list PID, the corresponding public key PKVi of Vi, and message signature tuples ððm1, σ1Þ, ðm2, σ2Þ, ,ðmn, σnÞÞ from Vi , respectively. The aggregate signature generator will generate signature σ; then it will transmit the tuple including the signature, the list PID, and time list T to the verifier.

(7) Aggregate Verify: In general, this algorithm is executed by another RSU. It takes an aggregating set V of n entities fV1, V2, ,Vng, the pseudo identity PI Di of each entity Vi . The verifier will check the time validity for each entity firstly. Then it will output true if the signature is valid or false

3.1. ELLIPTIC CURVE CRYPTOGRAPHY

As widely used in the cryptographic, the elliptic curve cryptography is an excellent algorithm which has an extremely high efficiency and a relatively excellent security. It can use much fewer bits to encrypt messages of the same length than the RSA algorithm in the field of public key cryptography. Because of its fewer calculation parameters, shorter bond length, and less time cost, the elliptic curve cryptography can be perfectly applied to application scenarios of VANETs. It was initially introduced by Miller [33]

ISBN: 978-81-955611-3-1

and Koblitz [34]. An elliptic curve E over a finite field Fp, where p is a large prime, is defined by the following equation:

$$y^2 = x^3 + ax + b(\mathrm{mod}\ p) \quad a, b \in F_p, \qquad (1)$$
$$\text{where } (4a^3 + 27b^2)\mathrm{mod}\ p \neq 0.$$

An infinity point *O* and all points (x,y) E form an additive cyclic group . Scalar multiplication over G is defines as

$$kP = P + P + \cdots + P \quad (k \text{ times}),$$

where P ∈ G

In recent years, Elliptic Curve Cryptography (ECC) has attracted wide attention. Under the same security level, ECC has many good properties, including smaller private key size, less computation, smaller storage amount and less bandwidth. It is generally believed that 224-bit elliptic curve guarantees the same level of security as 2048-bit RSA. Therefore, the signature scheme based on elliptic curve is more proper for low power devices. It is a practical and meaningful method to use elliptic curve signature scheme to achieve data integrity and identity authentication in the resource-constrained IoT environment

3.2 FORKING LEMMA Suppose that A is a probabilistic polynomial time Turing machine, and its input includes public data. We use Q and R to symbolize the number of queries that A can ask to the random oracle and the number of queries that A can ask to the signer, respectively. Suppose that over a period of time T, A can generate a legitimate signature ðm, σ1, h, σ2Þ within probability ε ≥ 10ðR + 1ÞðR + QÞ/2k. If someone do not know the private key, but successfully forge the signature ðσ1, h, σ2Þ with an indistinguishable distribution probability, then we can imagine a machine, which can get the secret information from the machine and obtain and replace the interaction with the signer by simulation. Eventually, it can generate two legitimate signatures ðm, σ1, h, σ2Þ and ðm, σ1, h′, σ2′Þ such that h ≠ h′ in expected time T′ ≥ 120686QT/ε.

4. CERTIFICATELESS AUTHENTICATION SCHEME VS PKI

Certificateless public key cryptography enables a similar functionality of public key infrastructure (PKI) and identity (ID) based cryptography without suffering from complicated certificate management in PKI or secret key escrow problem in ID-based cryptography. This Scheme avoids the inherent

ISBN: 978-81-955611-3-1

escrow of identity-based cryptography and yet which does not require certificates to guarantee the authenticity of public keys. The lack of certificates and the presence of an adversary who has access to a master key necessitates the careful development of a new security model which saves computation cost and communication overhead. It also utilises the benefits of aggregate signatures. Aggregate signature can combine *n* signatures on *n* messages from *n* users into a single short signature, and the resulting signature can convince the verifier that the *n* users indeed signed the *n* corresponding messages. This feature makes aggregate signature very useful especially in environments with low band width communication, low storage and low computability since it greatly reduces the total signature length and verification cost. This scheme does not only meet the privacy and security requirements for VANETs, but supports batch verification, autonomy, and conditional privacy preservation. Therefore, the certificateless aggregate signature (CLAS) scheme is particularly well suited to address secure routing authentication issues in resource- constrained vehicular ad hoc networks.

5. SHORTFALL

Since real application scenarios of VANETs require high efficiency, an efficient certificateless-based anonymous authentication and aggregate signature schemes are being developed. Unfortunately, most existing CLAS schemes have been found to have security flaws or have unsatisfactory performance in computation and communication costs. The low efficiency caused by the illegitimate signature in the aggregate verification process is one shortfall on which the work requires to be done in the future.

CONCLUSION

Future work could include the development of scheme which decreases latency, average delay and improves throughput using network simulators, such as OMNeT++, and road traffic simulators, such as SUMO. Besides, the future work will also includethe design of an authentication scheme based in 5G-enabled vehicular networks. It is imperative to develop a CLAS scheme that is robust against all types of attacks, which makes it more suitable for performing secure routing in resource-constrained VANETs.

REFERENCES

[1] Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad hoc networks. IEEE Trans. Dependable Secur. Comput. 2019, 18, 722–735. [CrossRef]

ISBN: 978-81-955611-3-1

[2] Alazzawi, M.A.; Chen, K.; Yassin, A.A.; Lu, H.; Abedi, F. Authentication and revocation scheme for VANETs based on Chinese remainder theorem. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1541–1547.

[3] Lloyd, D. Reported Road Casualties in Great Britain: Main Results 2015. 2016. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/533293/rrcgb-main-results-2015.pdf (accessed on 19 January 2022).

[4] Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. Sensors 2021, 21, 8206. [CrossRef]

[5] Aung, N.; Zhang, W.; Dhelim, S.; Ai, Y. Accident prediction system based on hidden markov model for vehicular ad hoc network in urban environments. Information 2018, 9, 311. [CrossRef]

[6] M. S. Kakkasageri and S. S. Manvi, "Information management in vehicular ad hoc networks: a review," Journal of Network and Computer Applications, vol. 39, pp. 334–350, 2014.

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

[8] Dedicated short range communications (DSRC)," 2018, http://grouper.ieee.org/groups/scc32/top_lvl3.html/.

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

[9] 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 IEEE INFOCOM—the 27th Conference on Computer Communications, pp. 1903– 1911, Washington, DC, USA, April 2008.

ISBN: 978-81-955611-3-1

[10]C. Zhang, X. Lin, R. Lu, and P. H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in Proceedings of IEEE International Conference on Communications, pp. 1451–1457, Beijing, China, May 2008

ISBN: 978-81-955611-3-1