

A survey on different privacy-preserving authentication schemes in VANET

Deepu Mathew

St. Joseph's College of Engineering and Technology, Palai

E-mail: vrossy.mathew608@gmail.com

Hima Anns Roy

St. Joseph's College of Engineering and Technology, Palai

E-mail: himaannsroy@gmail.com

Abstract. A vehicular ad hoc network(VANET) system used in modern transportation system that improves the road safety and other efficiency parameters. In this technology it uses cars as node in a network to develop a mobile network. In vanet, the distance between cars around 100 to 300 meters and only those ones are allowed to connect together. The broadcast of messages by vehicles are in an open-access environment. It makes several critical security issues. A mishandling of this information may cause several critical issues like traffic accident and other traffic problems. So authentication of vehicles is necessary to improve the safety in vanet. During authentication a vehicles confidentiality-related data, such as identity of user and information about locations must be kept private. There are different types of authentication schemes are available and preserving the privacy related data of vehicles are different in different authentication schemes. This survey aims to find the better schemes for privacy preserved authentication methods in the VANET system.

Keywords:CRL(Certification Revocation List),RSU(Road Side Unit),TA(Trusted Authority).

1. Introduction

Related to road security Vehicular ad hoc network (VANET) is one of the popular concept applications in many countries. It is an important part of the modern transportation systems. The aim of Vehicular Ad Hoc Network (VANET) is that to provide the road safety and comfort by decreasing the congestion in roads. In a VANET, each vehicle is use an on-board unit (OBU) and road-side units (RSU) installed at road side. A trusted authority (TA) is installed in background and other application servers are also running in back ground for supporting the proper working of the system. Communication between OBUs and RSUs is done by using a dedicated short range communications protocol using wireless channel. RSUs, TA, and other application servers are communicate with each other using a fixed secure network, Internet.

VANET offers secure driving experience and road safety, and other traffic related services. The basic use of a VANET is to grant vehicles to broadcast secure messages , message contains information like vehicular speed, traffic accident information to other nearby vehicles. This method of communication is called as vehicle2vehicle or V2V communications



and communication between vehicle and RSUs is known as vehicle2infrastructure or V2I communications.

The broadcasting of messages in an open-access network may cause security and privacy critical and other issues in the VANET. A mishandling of this message may cause to a traffic accident and loss of human lives, therefore vehicle authentication is an important part in this system. Therefore the main aim of designer is to make VANET more and more secure. During authentication time a vehicles privacy-related data, such as personal information and information about the location must be kept private. There are different types of authentication schemes are available and preserving the privacy related data of vehicles are different in different authentication schemes.

2. Related Works

In the last few years, many privacy preserving authentication methods have been proposed such as pseudonym based methods , group signature-based schemes, ID-based schemes, symmetric cryptography-based methods.

2.1. Pseudonym based schemes

Message authenticity is compulsory to defend VANETs from outsiders, as well as bad insiders. But since safety messages will not contain any responsive information, confidentiality is not mandatory .As a result, the transferring of safety messages in a VANET requires authentication but not encryption. Digital signatures are a good methods in the VANET setting, because safety related messages are normally standalone, and should be transform to receivers as fast as possible. A work by Raya and Hubaux [8], in which they described the safety and privacy requirements for VANET and suggest one of the initial pseudonym-based schemes, many other authors have followed their work and proposed a lot of pseudonym based and group signature-based schemes. The pseudonyms-based schemes are implemented by using Public Key Infrastructure (PKI). PKI based certificates are attached with the message that are signed with the equivalent private keys. Each certificate contains a pseudo identity. The relation between the pseudo identity and the certificate is known to the issuing authority, called certification authority (CA).

Raya et al. [2] introduce a hardware security module (HSM) or a Temper Proof Device (TPD) that is used to protected the cryptographic stuff stored in a vehicles OBU. This scheme suffer from the storage and communication overhead of pseudonymous certificates. Usage of Certification Revocation List(CRL) is a major drawback of this method. When revoking a vehicle, all the certificates issued to that vehicle needed to be included in the CRL whose size grows exponentially. Therefore, there is an extra overhead included in the distribution, storage and checking of CRL.

Zhang et al. [3] recently proposed a better scheme that requires a realistic TPD in its place of an ideal TPD. This method also provides conditional anonymity. Sun et al. [4] try to reduce the CRL by introducing a hash chains and use a proxy re-signature scheme in order to advance the time needed for update the CRL.

Lu et al. [5] propose a conditional privacy preserving approach. A vehicle wants to get short-time pseudonym keys from RSU and therefore, this method requires pervasive operation of RSUs. A major drawback of this system is that the trusted authority needs to frequently distribute the RSUs with updated CRL.

Rajput et al. [6] proposed a hierarchical pseudonymous-related method that requires vehicle to get primary pseudonym from the CA and secondary pseudonyms from the RSU. However, their method assumes the pervasive implementation of RSUs.

The approaches presented in [7] and [1] use identity based cryptography [9] where the public key is a recognizable identity and the equivalent secret key is generated by a Trusted Authority (TA). In order to provide privacy, the identifiable identity is concealed with the assist of a pseudonym and therefore, these schemes suffer from the pseudonym management overhead.

Zhang et al.[8] introduce a method that describes an identity based verification scheme that provide pseudo identity based certificates and the secret keys with the help of a TPD.

2.2. Group signature based scheme

In group signature method schemes [10],[11],[12] a vehicles real identity is concealed among a group of vehicles. The vehicles in a group sign messages with individual private keys and the receiver verifies the message with the groups public key. In case of a harmful message, the group manager is clever to trace the malicious member and later revokes it. Calandriello et al. [11] proposed a method that integrates both the group signature-based and pseudonymous-based schemes. However, the scheme is computationally costly as it needs to check a message against the blocked vehicles. Xiong et al. [14] use revocable ring signatures invented by Liu et al. [13]. The scheme describes conditional anonymity but suffers from the sharing of revocation information to all the vehicles. The important works in the area of privacy preserved authentication schemes in VANET are listed in the table1 along with the key results of that works.

Table 1. Title and Key Results in the area of authentication schemes in VANET.

Sno	Title	KeyResults
1	Security of Vehicular Ad Hoc Networks	Earliest pseudonym-based scheme
2	Secure vehicular communications	Hardware Security, Temper Proof
3	Distributed privacy-preserving authentication in VANET	Realistic TPD
4	Efficient pseudonyms Validation For vehicular communication	Hash chains, proxy re-signature
5	ECPP-secure vehicular communication	Short-time pseudonym keys
6	Hierarchical privacy preserving protocol-VANET	Primary and secondary pseudonyms
7	Scalable robust authentication protocol- vehicular comm.	RSUs to act as group managers

3. Comparison of different methods

Pseudonym scheme and group signature methods are the two main schemes in the area of privacy preserved authentication in VANET. The work done by Raya and Hubaux [4] is the first work proposes the pseudonym based scheme. This work use Public key infrastructure scheme.CA. Raya et al. [2] come up with more improvements by introducing a hardware security module (HSM) or a Temper Proof Device (TPD) that is used to protect the cryptographic content stored in a vehicles OBU. This work is more efficient than their previous works. Usage of HSM and TPD increases the efficiency of the system. But the system is suffered in the case that there is more overhead involved in the distribution and storage of pseudonym certificates. Certificate Revocation List usage is another major drawback of this system.

Zhang et al.[3] introduced realistic TPD in place of an ideal TPD which overcome the disadvantages of work done by CA. Raya et al. [2]. The usage of realistic TPD improves the overall working of the system. The scheme also offers conditional anonymity. The time required to update the CRL is one of the main problem faced by the works done in this area. The work by Sun et al. [4] reduces the CRL by proposing hash chains and uses a proxy re-signature scheme in order to get better the time required to renew the CRL. The work by Lu et al. [5] , the concept of short-time pseudonym keys requirement have some disadvantages that is the trustworthy authority needs to regularly issue the RSUs with updated CRL.Hierarchical pseudonymous-based approach that requires vehicle to get principal pseudonym from the CA and secondary pseudonyms from the RSU. But this system a pervasive use of RSUs is needed.

In the case group signature based methods in all works the vehicles real identity is concealed among a group of vehicles. The approach in [12] uses the RSUs to work as group managers in order to supervise and maintain the vehicles. In this work the main concept is that a group manager who have the central control to manage and maintain vehicles. The pervasive RSU deployment is need in this case but it can have a depressing impact on the overall performance. The scheme in the work by Liu et al. [13] provides conditional anonymity but suffers from the delivery of revocation list information to all the vehicles.

4. Results and Conclusion

The survey reveals that the pseudonym based schemes mainly suffer from the storage, communicational, computational overhead because of the usage of CRL. The number of vehicles revoked is more, CRL is increment exponentially. The group signature-based schemes suffer the overhead related to group management. Another disadvantage is the trust related problems with the vehicle acting as a group manager. The group signature based methods also have problems like computational overhead in terms of pairing-based calculations.

So the proper usage of a hybrid method that combines both two methods may leads to a better system which overcome the issues in each individual method.

5. References

- [1] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, Privacypreserving vehicular communication authentication with hierarchical aggregation and fast response, *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 25622574, Aug. 2016.
- [2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications, *IEEE Wireless Commun.*, vol.13, no.5, pp.815, Oct.2006
- [3] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516526, Mar. 2017.
- [4] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, An efcient pseudonymous authentication scheme with strong privacy preservation for vehicula rcommunications, *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 35893603, Sep. 2010.
- [5] R.Lu, X.Lin, H.Zhu, P.-H.Ho, and X.Shen,ECPP:Eficient conditional privacy preservation protocol for secure vehicular communications, in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1229123
- [6] U. Rajput, F. Abbas, and H. Oh, A hierarchical privacy preserving pseudonymous authentication protocol for VANET, *IEEE Access*, vol. 4, pp. 77707784, 2016.
- [7] J. Li, H. Lu, and M. Guizani, ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs, *IEEE Trans. Parallel Distrib. Syst.*, vol.26, no.4, pp.938948, Apr. 2015.
- [8] M.Rayaand , J.P.Hubaux,Securingvehicularad hoc networks, *J.Comput. Secur.*, vol. 15, no. 1, pp. 3968, 2007.
- [9] A. Shamir, Identity-based crypto systems and signature schemes, in *Advances in Cryptology*. Berlin, Germany: Springer, 1984, pp. 4753.
- [10] Lin, X. Sun, P.-H. Ho, and X. Shen, GSIS: A secure and privacypreserving protocol for vehicular communications, *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 34423456, Nov.2007.

- [11] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET, in Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw., 2007, pp. 1928.
- [12] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 16061617, May 2010.
- [13] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, Revocable ring signature, J. Comput. Sci. Technol., vol. 22, no. 6, pp. 785794, Nov. 2007.
- [14] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, Efficient and spontaneous privacy-preserving protocol for secure vehicular communication, in Proc. IEEE Int. Conf. Commun., May 2010, pp. 16.