An EMAP Based Vehicle to Grid Communication

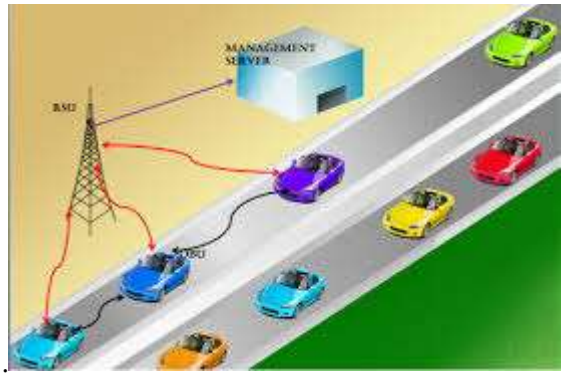
Manoj Kumar .A
Praveen Kanna .M
Pannai College Of Engineering And Technology

ABSTRACT

In this paper we investigate the revocation checking process in EMAP using a keyed Hash Message authentication Code(HMAC) where the key used in calculating the HMAC is shared only between non revoked On-Board Units (OBUs). Here implementing Cluster Based method , Due to large vehicles equipped in this field we are going to divide it in cluster format and then include the Expedite Message Authentication protocol for less time consuming process. Certificate revocation list is provided to check the correct news for the message received. This will help us to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, Expedite Message Authentication Protocol is considered to be more secure and efficient. In this by Clustering method , Time consuming is very low, so that message loss ratio get reduced.

INTRODUCTION

VEHICULAR ad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates



In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on the received message. The first part of the authentication, which checks the revocation status of the sender in a CRL, may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons:

1) To preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external

eavesdropper each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size.

LITERATURE SURVEY

In [1].we propose an efficient distributed certificate- service (DCS) scheme for vehicular networks. The proposed scheme offers flexible interoperability for certificate service in heterogeneous administrative authorities and an efficient way for any onboard units (OBUs) to update its certificate from the available infrastructure roadside units (RSUs) in a timely manner. In addition, the DCS scheme introduces an aggregate batch verification technique for authenticating certificate-based signatures, which significantly decreases the verification overhead. Security analysis and performance evaluation demonstrate that the DCS scheme can reduce the complexity of certificate management and achieve excellent security and efficiency for vehicular communications.

In [2], we propose an efficient pseudonymous authentication scheme with strong privacy preservation (PASS), for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of the certificate revocation list (CRL) in PASS is linear with the number of revoked vehicles and unrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports the roadside unit (RSU)-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost unrelated to the number of updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle, even though all RSUs have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported schemes in terms of the revocation cost and the certificate updating overhead.
In [3], As a prime target of the quality of privacy in vehicular ad hoc networks (VANETs), location privacy is imperative for VANETs to fully flourish. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. To cope with the issue, in this paper, we present an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. In particular, we first introduce the social spots where several vehicles may gather, e.g., a road intersection when the traffic light turns red or a free parking lot near a shopping mall.

SYSTEM DESIGN

In VANETs, the primary security requirements are identified as entity authentication, message integrity, nonrepudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirementsIn this paper, we propose an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. EMAP employs keyed Hash Message Authentication Code ðHMACÞ in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs. In addition, EMAP is free from the falsepositive property which is common for lookup hash tables as it will be indicated in the next section. We have proposed EMAP for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed EMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, EMAP has a modular feature rendering it integrable with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL

CONCLUSION

Security is the major issue to implement the VANET. In this article we study the security requirements and challenges to implement the security measure in the VANET. Different types of attacks and their solutions are also discussed. We discuss some technologies which are used in thedifferent solutions. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in the VANET because generally packets on the

network do not contain any confidential data.

REFERENCES

[1] S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004

[2] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[3] YaseerToor et al., "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3,pp. 74-88.

[4] Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006; http://www.crhc.uiuc.edu/~yihchun/

[5] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21

[6] Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171

[7] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.

[8] Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011).

[9] Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", Proceeding of IEEE ICNP 2002, pp 78-87, Nov 2002.

[10] Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B. V. , pp 175-192, 2003

[11] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Network", ACM Workshop on Wireless Security, San Diego , CA, September 2003.

[12] Fasbender, D. Kesdogan and O. Kubitz, "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE VTS, 46th Vehicular Technology Conference, USA, 1996.

[13] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCom'02, pp. 23-26,2002

[14] Fonseca and A. Festag, "A survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", NEC Network Laboratories, 2006.

[15] Xiaodong Lin et al., "Security in Vehicular Ad Hoc Network", IEEE communications magazine, April 2008, pp. 88-95

[16] Menezes, S. Vanstone, and D. Hankerson, "Guide to elliptic curve cryptography", Springer Professional Computing (Springer, New York 2004).

[17] J. Hof fstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem", Lecture Notes in Computer Science, Vol. 1423, 1998, pp 267-288.