Performance and Scalability Assessment for Non-Certificate-Based Public Key Management in VANETs

Pei-Yuan Shen, Queensland University of Technology, Australia
Maolin Tang, Queensland University of Technology, Australia
Vicky Liu, Queensland University of Technology, Australia
William Caelli, Queensland University of Technology, Australia

ABSTRACT

Current research in secure messaging for Vehicular Ad hoc Networks (VANETs) focuses on employing a digital certificate-based Public Key Cryptosystem (PKC) to support security. However, the security overhead of such a scheme creates a transmission delay and introduces a time-consuming verification process to VANET communications. This paper proposes a non-certificate-based public key management for VANETs. A comprehensive evaluation of performance and scalability of the proposed public key management regime is presented, which is compared with a certificate-based PKC by employing a number of quantified analyses and simulations. In this paper, the authors demonstrate that the proposal can maintain security and assert that it can improve overall performance and scalability at a lower cost, compared with certificate-based PKC. The proposed scheme adds a new dimension to key management and verification services for VANETs.

Keywords: Non-Certificate-Based Public Key Management, Public Key Registry (PKR), Secure Messaging in VANETs, System Design for VANETs, Vehicular Ad hoc Networks (VANETs)

INTRODUCTION

Recently, there has been an increase in research concerned with the development of vehicular communications technologies. These technologies are widely known as Vehicular Ad hoc Networks (VANETs). Primarily, VANETs are designed to distribute safety-related messages and to disseminate traffic condition information to enhance road safety. A digital certificate-based Public Key Cryptosystem (PKC) is the major securing method proposed to support secure messaging in VANETs (Institute of Electrical and Electronics Engineers, 2006). This paper asks: Does the use of the certificate-based PKC present an efficient solution for secure messag-
ing for VANETs? While a certificate-based PKC may seem to be a common scheme to support security services in electronic communication environments there is still a lack of successful large-scale, certificate-based PKC deployment in the world.

Obviously, the major shortcoming of relying on a certificate-based PKC to support security for any large-scale environment (including VANETs) involves the high cost of maintaining certification and the time-consuming certification verification process. It is, therefore, seen as impractical to deploy such a certificate-based PKC approach to support security for VANETs. Such a scheme can create transmission delay and introduce a time-consuming certificate verification process to VANET communications, including revocation tests; this would defeat the purpose of using VANETs to improve road safety.

In our previous paper (Shen et al., 2011), we propose a non-certificate-based public key management regime – the Public Key Registry (PKR) for VANETs. The aim of the proposed PKR regime is to operate public key management and verification without certification in VANETs. Compared to the certificate-based PKC, this new approach can not only maintain security with improved performance and scalability, but also reduce the security overhead of message transmission. This paper aims to provide a comprehensive evaluation of performance and scalability of the proposed PKR regime, which is then compared to a certificate-based PKC, by performing a number of appropriate simulations.

To the best of our knowledge, the proposed PKR regime is the first to manage public keys by employing a centralised directory without certification for VANETs. This research also improves scalability and performance for VANETs, compared to the certificate-based PKC.

RELATED WORK

Certificate-Based PKC Scheme in VANETs

Numerous studies and standards cite the use of a certificate-based PKC to support security for VANETs (Di Crescenzo et al., 2007; Freudiger et al., 2007, 2008; Institute of Electrical and Electronics Engineers, 2006; Iyer et al., 2008; Kounga et al., 2009; Papadimitratos et al., 2007; Plößl & Federrath, 2008; Plößl et al., 2006; Rao et al., 2007; Raya & Hubaux, 2005a, 2005b, 2007; Raya et al., 2006; Sunnadkal et al., 2010; Wang et al., 2008; Xiaonan et al., 2007). For example, Raya and Hubaux (2005a) appear to be the first research team to propose a vehicular Public Key Infrastructure (PKI), based on a certificate-based PKC scheme to support security services for message exchange in the vehicular communication environment. IEEE 1609.2-2006 Standard for Wireless Access in Vehicular Environments (WAVE) (2006) mandates the use of certificate-based PKC mechanisms to support authentication and encryption services for VANETs. Papadimitratos et al. (2007) discuss a security architecture based on the certificate-based PKC mechanism for VANETs. However, only a few authors have acknowledged the shortcomings of using the certificate-based PKC scheme in VANETs (Plößl & Federrath, 2008; Raya & Hubaux, 2007). Secure messaging based on the certificate-based PKC scheme has a number of limitations, including complexity in certificate verification and management, scalability, performance in a large-scale environment, and timely access to certificate revocation information. These issues with the certificate-based PKC scheme remain when applied to VANETs.
Implementation of Improved Hash and Mapping Modified Low Power Parallel Bloom Filter Design
www.igi-global.com/article/implementation-of-improved-hash-and-mapping-modified-low-power-parallel-bloom-filter-design/111273?camid=4v1a

Human and Social Aspects of Password Authentication
www.igi-global.com/chapter/human-social-aspects-password-authentication/29042?camid=4v1a