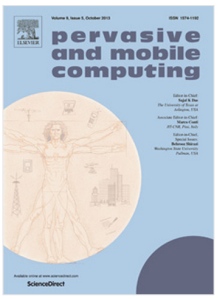
Accepted Manuscript



Secure authentication framework for cloud-based toll payment message dissemination over ubiquitous VANETs

Qamas Gul Khan Safi, Senlin Luo, Limin Pan, Wangtong Liu, Guangluo Yan

PII: S1574-1192(17)30193-1
DOI: https://doi.org/10.1016/j.pmcj.2018.05.004
Reference: PMCJ 935

To appear in: *Pervasive and Mobile Computing*

Received date : 22 April 2017
Revised date : 8 March 2018
Accepted date : 21 May 2018

Please cite this article as: Q.G.K. Safi, S. Luo, L. Pan, W. Liu, G. Yan, Secure authentication framework for cloud-based toll payment message dissemination over ubiquitous VANETs, *Pervasive and Mobile Computing* (2018), https://doi.org/10.1016/j.pmcj.2018.05.004

Secure authentication framework for cloud-based toll payment message dissemination over ubiquitous VANETs

Qamas Gul Khan Safi, Senlin Luo, Limin Pan*, Wangtong Liu and Guangluo Yan
Information System & Security and Countermeasures Experiments Center, School of Information and Electronics, Beijing Institute of Technology, 100081, P.R. China.
*pan.limin@yahoo.com

Abstract

The privacy and security issues of information message dissemination have been well researched in typical VANETs. However, cloud computing paradigm is merely utilized for secure information message dissemination over VANETs. In this paper, we propose a secure authentication framework for cloud-based toll payment message dissemination over ubiquitous VANETs, which primarily deal with two types of information messages that is general purpose and special purpose information messages. General purpose information messages include infotainment, traffic congestion, location-based services and emergency services. While the special purpose information messages include toll tax and revenue collection services. Moreover, our secure authentication framework (CCES-PKC) integrates the novel cloud-based pairing-free certificate-less encryption, secure authentication control, signature-based information encryption, decryption through cloud verification and signature authentication along with batch auditing. The certificate overhead management is passed over to the cloud infrastructure for fine-grained information message dissemination by enabling verification, integrity and confidentiality. Performance assessments including efficiency, security and experimental analysis emphasize that the proposed scheme is remarkably appropriate for secure toll payment information message dissemination.

Keywords

Cloud computing, VANETs, Authentication, Toll payment, Encryption, Signature verification

1 Introduction

Cloud computing is a promising paradigm as it influences the development process of cloud-oriented applications, networking and communication technologies. Cloud computing provides inexpensive, flexible and on-demand services. Many companies such as Google, Microsoft, Amazon, AT&T, Salesforce.com and Rackspace are offering cloud services and solutions. Cloud computing is dynamic and robust but there are various security and privacy concerns regarding data and users [1].

VANETs (Vehicular ad-hoc networks) is another auspicious technology for providing effective and dynamic solutions for traffic management, secure navigational services, vehicular safety and infotainment [2]. On the other hand, the automobile industry is introducing the new vehicles equipped with more cutting-edge technologies and powerful computing resources [3]. All these technologies spark the development process of valuable applications for intelligent transportation service (ITS) [4]. The primary objective of these applications is to enhance efficiency, convenience and driving safety. The innovative intelligent driver-less vehicles are also in need of more and more connectivity for information sharing between cloud infrastructure, vehicular nodes and the roadside infrastructure [5]. These Vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) [6] based applications not only bring new