Information Sciences 317 (2015) 48–66

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks ☆

Shi-Jinn Horng [a,b,*], Shiang-Feng Tzeng [b], Po-Hsian Huang [c], Xian Wang [a], Tianrui Li [a], Muhammad Khurram Khan [d]

[a] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China
[b] Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan
[c] Department of Applied Digital Media, Jen-Teh Junior College of Medicine, Nursing & Management, Miaoli County 35564, Taiwan
[d] Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Received 3 August 2013
Received in revised form 13 April 2015
Accepted 16 April 2015
Available online 24 April 2015

Keywords:
Aggregate signature
Authentication
Certificateless public key cryptography
Privacy
Vehicular ad hoc networks

ABSTRACT

Certificateless public key cryptography was introduced to solve the complicated certificate management problem in traditional public key cryptography and the key escrow problem in identity-based cryptography. The aggregate signature concept is useful in special areas where the signatures on many different messages generated by many different users need to be compressed. This feature is very attractive for authentication in a resource constrained environment because it allows large bandwidth and computation time savings. This paper proposes a new certificateless signature scheme. A new certificateless aggregate signature scheme for vehicle-to-infrastructure communication in vehicular ad hoc networks based on the new certificateless signature scheme is presented. We demonstrate that the proposed certificateless aggregate signature scheme can also achieve conditional privacy preservation, in which each traffic message launched by a vehicle is mapped to a distinct pseudo identity. A legal authority can retrieve the real identity from any pseudo identity for any dispute event. In addition, the proposed scheme is provably secure against existential forgery on adaptively chosen message attack in the random oracle model assuming the computational Diffie–Hellman problem is hard. Furthermore, the proposed scheme presents efficient computational overhead with the existing well-known schemes and is suitable for practical use.

1. Introduction

The state-of-the-art wireless communication technologies have been used to expedite the intelligent transportation system [40]. For the last few years, vehicular ad hoc networks (VANETs) have become a significant research area due to its specific features and applications such as road safety and traffic management. Such traffic sensing and collecting related

☆ This work was supported in part by the Ministry of Science and Technology under Contract Nos. 103-2221-E-011-128- and 103-2218-E-011-014-, and it was also partially supported by the 111 Project under the grant No. 111-2-1 and One Hundred Talents Program 2012, Sichuan Province.

* Corresponding author at: Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan. Tel.: +886 2 27376700.

E-mail addresses: horngsj@yahoo.com.tw (S.-J. Horng), sftzeng@gmail.com (S.-F. Tzeng), phhuang@jente.edu.tw (P.-H. Huang), drwangxian@gmail.com (X. Wang), trli@swjtu.edu.cn (T. Li), mkhurram@ksu.edu.sa (M.K. Khan).

http://dx.doi.org/10.1016/j.ins.2015.04.033
0020-0255/

information simply turns a VANET into a vehicular sensor network (VSN) [25], which has emerged as a new application scenario that has innovated transportation safety, traffic flow control and the user's driving experience [30].

In VANETs the mobile nodes are vehicles such as cars, buses, trucks and motorcycles that do not rely on a predefined or centralized infrastructure to keep the network connected as with mobile ad hoc networks (MANETs) [46]. However, vehicles are not an issue with limited power, space and computing ability restrictions normally adopted for MANETs. More challenging is the node high speed (more than 36 km/h [3]) movement, the large scale and number of nodes (up to 100 nodes) in VANETs. Due to the high speed mobility, the communication delay should be short enough to meet the stringent time requirement [47].

A VANET consists of trusted authorities (TAs), road side units (RSUs) along the roads and on board units (OBUs) installed in the vehicles. According to the dedicated short range communications (DSRC) [1] protocol, vehicles broadcast traffic related messages every 100–300 ms, which maintains the vehicles' driving related information, such as current time, location, driving status and traffic events, to other vehicles. With multi-hop forwarding, the messages will be either terminated by an RSU or dropped when they exceed their lifetime. When receiving messages an RSU can either forward the messages to a traffic control center if the messages are considered to contain possible valuable information, or react to them if the sending vehicles for the messages are nearby with some demands that can be responded locally. With all of the related collected traffic information, the traffic control center can obtain better awareness of the traffic environment and analyze an optimized management strategy for traffic load control.

Before putting the aforementioned promising applications into practice in VANETs we must ensure both security and privacy issues. In general, the users do not want their sensitive information such as real identities to be exposed to protect themselves against any unlawful tracing and user profiling. On the other hand, when a traffic collision or crime occurs, the legal authorities should be able to retrieve or trace vehicle messages by revealing their identities, which is the so called conditional privacy. Thus, privacy must be preserved and conditional.

Authentication is a crucial security issue for VANETs. Many authentication mechanisms have been proposed over the past few years using public key infrastructure (PKI)-based or identity (ID)-based authentication. Authentication mechanisms based on PKI have been presented in [3,28,32–34,38], but the system availability is still infeasible. PKI-based authentication mechanisms require a certificate authority to maintain a pool of certificates for vehicle public keys and RSUs or vehicles need additional computation to verify the certificates of others. Although many ID-based authentication mechanisms have been proposed to solve the computation and communication overhead, these mechanisms are considered suitable only for private networks [36] because of the key escrow problem. Xiong et al. [42] recently proposed a certificateless aggregate signature (CLAS) scheme based on certificateless public key cryptography, which is suitable for ad hoc networks. The security of such a scheme is theoretically proven. Unfortunately, He et al. [16] pointed out that an adversary could forge a legal signature for any message against Xiong et al.'s CLAS scheme. He et al. did not provide any countermeasure to enhance the security.

This paper presents a new certificateless signature (CLS) scheme. A new CLAS scheme for vehicle-to-infrastructure (V2I) communication in vehicular ad hoc networks (VANETs) based on the new CLS scheme is then proposed. By using the CLAS for authentication our scheme may suppress the inherent key escrow property of ID-based cryptosystem without losing their most attractive advantage which is the absence of vehicle certificates and the necessary management overhead. The contributions of this work are as follows. We designed a novel CLAS scheme as the cryptographic primitive, which is efficient and provably secure against existential forgery on adaptively chosen message attacks in the random oracle model by assuming that the computational Diffie–Hellman (CDH) problem is intractable. Second, our scheme can achieve conditional privacy-preservation, in which each message launched by a vehicle is mapped to a distinct pseudo identity, while a legal authority can retrieve the real identity of a vehicle from any pseudo identity. Third, the verification procedure in our scheme needs only a small constant number of pairing computations, independent of the number of aggregated signatures. Compared to previous CLAS schemes our scheme is efficient in computational cost. In addition, the proposed scheme can make the message verification in VANETs more suitable for practical use.

The remainder of this paper is organized as follows. A survey of related works is provided in Section 2. In Section 3, a brief review of some basic concepts and security notions used in our scheme is given, including the pairing technique, system model, scheme framework and security notions. In Section 4, we propose a novel CLAS scheme for secure V2I communications and give its security proof in the random oracle model under the CDH problem. In Section 5, the approach of batch verification is discussed. In Section 6, we give security analysis and performance evaluation for our scheme. Finally, we conclude the paper in Section 7.

2. Related works

The digital signature [39] provides message authentication, integrity and non-repudiation properties. Anyone can check the validity of the signature by knowing the public key of the signer. This characteristic enables the digital signature to be applied efficiently to one-to-one (unicast) and one-to-many (multicast) applications. Some multicast applications may need the root node to collect messages from leaf nodes, which results into a many-to-one communication [29,48]. When many leaf nodes send messages simultaneously, the root node could be swamped. For example, from the V2I communications in VANETs [37,47], each RSU or traffic control center needs to verify a large number of messages in a high density traffic scenario. This will lead to a high computation burden. Sometimes we have to work in environments with low bandwidth