Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Secure authentication in motion: A novel online payment framework for drive-thru Internet

Jun Song, Fan Yang, Lizhe Wang*

School of Computer Science, China University of Geosciences, Wuhan, 430074, PR China

HIGHLIGHTS

- We propose a novel secure payment framework for the drive-thru Internet.
- We present an adaptive authentication scheme in online and offline scenarios.
- Utilizing a new certificateless public key scheme will derive a novel property.
- A traceable batch authentication will reduce the load of key computation and management.
- It provides a comprehensive evaluation to show the security and feasibility of the proposed scheme.

ARTICLE INFO

Article history:
Received 1 September 2015
Received in revised form
29 December 2015
Accepted 16 June 2016
Available online xxxx

Keywords:
Drive-thru Internet
Online payment
Auditing
Encrypted signature

ABSTRACT

The security and privacy issues have been well investigated in typical vehicle ad hoc networks. However, considering the drive-thru Internet properties, in particular for a secure and in-motion payment services case, merely implementing the existing online payment schemes may be either infeasible or inefficient. In this paper, we propose an advanced online payment framework, which integrates three main features, including the novel pairing-free certificateless encryption, signature and semi-honest RSU-aided verification, and the CA-aided tracking and batch auditing, and providing following properties independently, e.g., achieving a higher trust level and supporting primary security services, introducing a semi-honest RSU to indicate more practicality, and optimizing the verifying and auditing efficiency for a large number of authentication requests case. Performance evaluations such as security analysis, efficiency analysis, and simulation evaluation show the security and feasibility of the proposed framework.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

With the advancement of vehicular ad hoc networks (VANETs) in recent years, increasing numbers of researchers and engineers have developed much new concepts and innovative ideas into the intelligent transportation services, *e.g., Toyota Safety Sense, BroadR-Reach Automated Compliance*, and *Mercedes-Benz Companion*, emerging as a promising approach to ensure a high quality of life. The primary purpose of vehicular networks is to enable vehicular communication applications, such as increasing driving safety, efficiency, and convenience [1,2]. However, people might prefer to get Internet services via driving vehicles quickly and easily, and to fully experience the pleasures of activities, such as online shopping, downloading software, and uploading video or audio, the so-called drive-thru Internet [3]. To meet these demands, it really needs to provide not only a *large-scale high-quality* deployments of wireless infrastructures, i.e., a stable and reliable communication environment, but a set of effective security mechanisms to secure vehicular communication.

Over the past several years, there have been much research on achieving an efficient message authentication [4,5] or establishing a secure communication channel [6,7] in typical VANETs. However, from the security and privacy perspectives, vehicular networks have brought many new challenges owing to network congestion and performance degradation issues, particularly when vehicular nodes are on the status of *intermittent* or *short-lived* communication connectivity [8,9], such as in a typical drive-thru Internet scenario. More exactly, compared with general wireless ad hoc networks, the drive-thru Internet in nature not only is an improvement of network property and user quantity, but also has some new features involved, i.e., fast-moving nature, intermittent network connectivity, and high contention environments, etc. In addition, it should be noted that, when a large number of fast-moving vehicle nodes compete for communication simultaneously, they

* Corresponding author.
E-mail address: lizhe.wang@gmail.com (L. Wang).

http://dx.doi.org/10.1016/j.future.2016.06.011
0167-739X/© 2016 Elsevier B.V. All rights reserved.

Please cite this article in press as: J. Song, et al., Secure authentication in motion: A novel online payment framework for drive-thru Internet, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.06.011

may have fallen into to a kind of *volatile* or *vulnerable* communications environment [8]. From the point of view of authentication protocol, if the access requests from vehicle nodes cannot submit to an authentication server or a secure gateway multiple times, those web-based secure services may be inefficient in such a case.

Although the security and privacy issues have been well investigated in typical vehicular ad hoc networks scenarios [1,2,10], most of them tend to focus on network environment with properties of good stability and high reliability. Generally, vehicular applications need security assurance to authenticate entities and trustworthy information exchange via an insecure network. Similar to the previous work [4,11,12], both authentication and identification are the fundamental mechanisms in securing VANETs. For the case of online payment over drive-thru Internet, it is essential to address higher security demands and goals for electronic transactions. Due to its in-motion payment nature, more security properties, i.e., confidentiality, integrity, authenticity, and non-repudiation, should be the most essential security concerns that must be provided. Considering these properties, existing online payment solutions, i.e., proposed for general static wireless networks, may be infeasible for the drive-thru Internet scenario.

To address above concerns, in this paper, we propose an advanced secure and efficient online payment framework especially for a drive-thru Internet applications. The contributions of this paper are threefold. First, inspired by *Lite-CA-based* public key cryptosystem [13], we propose a new pairing-free certificateless encryption scheme, which is not only to reduce the certificate management complexity but to achieve a higher trust level as well, *e.g.*, to achieve an explicit authentication property. Second, based on the proposed encryption and signature scheme, we introduce an RSU-aided online verification process, especially considering a more practical security property, i.e., the semi-honest RSUs, and thus appropriate for the secure online payment applications in drive-thru Internet case. Third, with the purpose to enhance the security of proposed framework, we present a CA-aided tracking and batch auditing scheme to improve the verifying and auditing efficiency in such a case, *e.g*, a large number of authentication requests. Besides that, a comprehensive performance based on drive-thru Internet scenario, including security analysis, efficiency analysis, and simulation and numerical analysis, is presented to show the security and feasibility of the proposed framework.

The rest of this paper is organized as follows. Section 2 presents the background and the related work, and overviews the related cryptographic requirements. Section 3 introduces the system model and security goals. Then, we present a formal definition and design of the proposed verifiably encrypted signature scheme without pairing in Section 4. Section 5 describes the detailed description of the secure online payment framework, including the system setup and different algorithms involved. Security analysis and performance evaluation are presented in Sections 6 and 7, respectively. Section 8 concludes the paper.

2. Background and related work

2.1. Related work

Security and privacy are always hot topics in VANETs [1,2,10]. [11] investigated the methods of providing security services and preserving privacy in VANET, especially to address two fundamental issues, *e.g.*, certificate revocation and conditional privacy preservation. [14] presented an RSU-aided messages authentication scheme to meet the needs of the messages authentication. In this scheme, RSU is trustworthy and hard to be compromised. Recent work [15] introduced a batch authentication scheme by utilizing pairing-based computation, to achieve the verification of lots of messages. Besides that, a recent work [16], proposed a stored-value card to provide an added-value service of payment in VANET. This work focused on a specific wireless network scenario. None of these solutions provides the online payment in case of drive-thru Internet, particularly for scenario where a lot of fast-moving vehicle nodes compete for communication simultaneously. Table 1 shows a quantitative comparison between the other relevant schemes and our schemes in terms of functions and features.

For the case of authenticated key agreement frameworks, so far there are many different categories of public key cryptosystem (PKCs), such as CA-based PKC [17], identity-based PKC (IBC) [18–20], certificateless (CL)-PKC [21,22], and *lite*-CA based PKC [13], and so on. Generally, in CA-based PKC schemes exist a most common issue, that is, *the complexity of certificates management*. Previous solutions of VANETs mainly adopt the ID-based authenticated key exchange (AKE) scheme [18,19,23], which reduces the management workloads of public key certificates compared with the CA-based PKC scheme. However, its *key escrow problem* still exists. [21] first introduces a certificateless (CL) public key cryptosystem, which usually exists *the impersonation attack issue* [13]. In addition, [13] introduced a *Lite-CA-Based* PKC scheme, which can be viewed as a *variations* originated from certificateless PKC (CL-PKC). This scheme achieves the highest trust level, i.e., detecting the impersonation attack easily, and provides efficient public key certificate management.

In this paper, we also propose a new certificateless public key encryption scheme, including two main properties: to resist the impersonation attack by introducing an explicit authentication mechanism, and to relieve the certificates management difficulty by utilizing a CL-PKC method as well. According to the existing results from [13], we discuss features and functions of various public key cryptosystems, and further show much more advantages of our proposed scheme, as shown in Table 2.

2.2. Security threats

The possible threats for an online payment framework include:

- **Message forging/cheating**: An adversary can send fake messages so as to either cheat on its identity, *e.g.*, Sybil attack, or disperse fake information, *e.g.*, forged payment receipts.
- **Message tampering**: An adversary may tamper the received messages and broadcast them to other nodes.
- **Message dropping**: An adversary may drop the messages to conduct a black-hole attack.
- **message congestion**: An adversary sends irrelevant bulk messages to take up the communication channel or to consume the service resources.
- **Message detour attack**: An adversary may take indirect or detour paths intentionally to increase services cost.
- **Message replay attack**: An adversary replays the expired messages in order to disturb the network.

3. System model and design goals

In this section, we present the system model and security goals towards an advanced online payment framework for drive-thru Internet.

3.1. System architecture

As shown in Fig. 1, the proposed secure online payment framework under consideration consists of five network entities: a root *certificate authority* (CA), a few of stationary *roadside units*

Download English Version:

https://daneshyari.com/en/article/4950308

Download Persian Version:

https://daneshyari.com/article/4950308

Daneshyari.com