Computer Communications 35 (2012) 188–195

Contents lists available at SciVerse ScienceDirect

Computer Communications

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

An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network

Wenmin Li *, Qiaoyan Wen, Qi Su, Zhengping Jin

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

Article history:
Received 12 November 2010
Received in revised form 3 September 2011
Accepted 5 September 2011
Available online 10 September 2011

Keywords:
Vehicular ad hoc network
Wireless communication
Security
Payment
Data volume transferred

ABSTRACT

Value-added applications in vehicular ad hoc network (VANET) come with the emergence of electronic trading. The restricted connectivity scenario in VANET, where the vehicle cannot communicate directly with the bank for authentication due to the lack of internet access, opens up new security challenges. Hence a secure payment protocol, which meets the additional requirements associated with VANET, is a must. In this paper, we propose an efficient and secure payment protocol that aims at the restricted connectivity scenario in VANET. The protocol applies self-certified key agreement to establish symmetric keys, which can be integrated with the payment phase. Thus both the computational cost and communication cost can be reduced. Moreover, the protocol can achieve fair exchange, user anonymity and payment security.

1. Introduction

Vehicular ad-hoc network (VANET), in which vehicles and roadside infrastructure constitute the nodes, aims to provide safety and comfort for drivers and passengers. Value-added applications in VANET, which improve passenger comfort and offer great business opportunities, attract more and more attention in our daily life. Most of such applications come with the emergence of electronic trading. Hence an efficient and secure payment protocol associated with the application scenario is a must.

Normally, how to design a mobile payment protocol depends on its associated scenarios which arise from vehicle-to-vehicle and vehicle-to-roadside communications in VANET. In [1], the authors demonstrated a restricted connectivity scenario (as shown in Fig. 1) for value-added applications, where the vehicle cannot communicate directly with the bank for authentication during a payment transaction due to the lack of internet access. In the described scenario, concrete applications divided into event-based applications and session-based applications. In event-based applications, vehicle's payment is reflected by one-time events, e.g. sending a message, querying traffic information, purchasing gas. In session-based applications, vehicle is charged based on data volume transferred, such as media downloading, map downloads and updates or on-line movies [2–4].

Therefore, the characteristics of different applications open up new challenges that must be considered by payment protocol designers to achieve a secure and efficient payment. To summarize, the following requirements should be addressed when designing a suitable payment protocol in VANETs [1,3,5,6]. First, the designed payment protocol should conform to the real communication scenario. Second, a payment protocol should be light-weight, that is, with low computational complexity and low communication overhead, so it can be easily performed. Third, fair exchange and user anonymity should be achieved. Finally, payment security, such as confidentiality, non-repudiation of origin, resistance to conventional attacks, and the avoidance of overspending and double spending, should be satisfied.

In this paper, we design a mobile payment protocol for applications in the restricted connectivity scenario of VANET, which attempts to meet these requirements. We apply the self-certified key agreement to generating the symmetric encryption keys, which combines the advantages of both public-key cryptography and symmetric-key cryptography. Our design guarantees that the session key is fresh in every payment of a payment transaction, which provides more robust security protection. The key agreement phase can be integrated with the payment phase which is far less complex. At the same time, due to using self-certified public keys (SCPKs) on elliptic curve, the protocol not only avoids the requirement of a large public key infrastructure (PKI) but also achieves efficient performance in contrast to other public key cryptosystems. Moreover, our protocol supports not only data volume transferred based application but also one-time event application.

The remainder of this paper is structured as follows. In Section 2, we introduce the related works. In Section 3, we present the preliminaries and notations used in the rest of the paper. In Section 4, we

* Corresponding author. Tel.: +86 10 62283240.
E-mail address: liwenmin02@hotmail.com (W. Li).

0140-3664/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2011.09.003

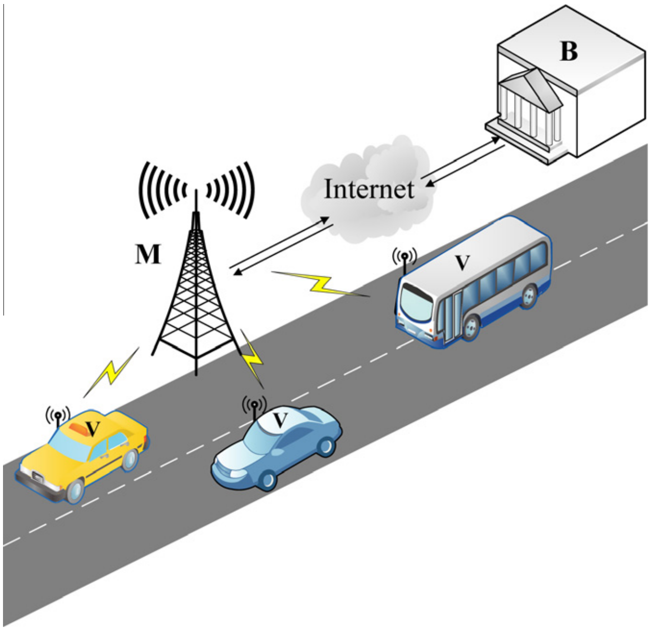

Fig. 1. The restricted connectivity scenario.

propose our mobile payment protocol for restricted connectivity scenarios in VANET. The security and performance analysis of the proposed protocol will be found in Section 5. Finally, conclusions are given in Section 6.

2. Related works

Over the past years, many academic papers are published to describe the mobile payment protocol. Among these protocols, [7] dedicated to unify many proposed m-commerce usage scenarios into a single framework, and then use this framework to analyze security issues. Later, as far as security concerned, several payment protocols [3,8,9] based upon PKI were proposed for wireless mobile networks. However,[10] pointed out that such protocols are not suitable for wireless mobile networks due to time consuming. To reduce the computation loads, they also presented an efficient and practical payment protocol for mobile commerce.

However, all these protocols are only suitable for full connectivity scenario where all the entities are directly connected one to another (as described in [7]). Designing mobile payment protocol suitable for restricted connectivity scenarios, achieving the same security and performance levels as the full connectivity scenario, is a challenge. Excellent protocols [1,11–13] constitute examples of mobile payment protocols suitable for scenarios with communication restrictions. However, such proposals do not satisfy requirements of applications based on either time spent or data volume transferred. The reason is that such applications require multiple payments in a payment transaction while the proposed protocols allow only one. Hence, these protocols are not suitable for session-based applications in the restricted connectivity scenario of VANET, which opens a new challenge to design protocol with multiple payments in one transaction.

3. Preliminaries

In this section, we briefly review the basic concepts on self-certified public keys (SCPKs) and some related mathematical problems. Besides, the symbols used in the rest of this paper are illustrated in Table 1.

Table 1
Notations.

ID_p	The identity of participant P
Pk_p	The public key of participant P
R_p	A witness for participant P
s_p	The secret key of participant P
$[M]_k$	Message M encrypted by symmetric key k
OI	Order information containing the price and order descriptions
H_i,f	The one-way hash function
SN	Serial number of the payment
InitRequest	
InitResponse	A request (response) for initiating conversation
AuthRequest	
AuthResponse	A request (response) for authentication
PRequest	
PResponse	A request (response) for payment
DRequest	
DResponse	A request (response) for redeeming tokens

3.1. Diffie–Hellman assumption

Choose elliptic curve E defined over a finite field F_q of characteristic p, and a base point $P \in E(F_q)$. The public elliptic curve domain parameters over F_q should be chosen appropriately to prevent the employment of any efficient algorithm from solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) or ECCDH in the cyclic subgroup (p). Let G be a cyclic additive group generated by P, whose order is a prime n. We consider the following problems in the additive group $(G,+)$ [14]:

Elliptic Curve Discrete Logarithm Problem: Given two group elements P and Q, find an integer $x \in Z_n^*$, such that $Q = xP$ whenever such an integer exists.
Elliptic Curve Decision Diffie–Hellman Problem: For $a,b,c \in Z_n^*$, given P, aP, bP, cP decide whether $c \equiv ab\ modq$.
Elliptic Curve Computational Diffie–Hellman Problem: For $a,b \in Z_n^*$, given P, aP, bP, compute abP.

Up to now, there is no efficient algorithm to be able to solve any of the above problems [15].

3.2. Self-certified public keys

A self-certified public keys combines the advantages of certificate-based and identity-based public key cryptosystems, and also provides a mechanism for authenticating a user's public key [16–18]. The public key of user is computed directly from the signature of the system authority (**SA**) on the user's identity. A simple self-certified scheme is presented below.

Set up: **SA** chooses a non-singular high elliptic curve E defined over a finite field F_q which is used with a based point generator P of prime order n. **SA** chooses a key pair (s_s,Pk_s), where $Pk_s = s_sP$. The related parameters E, P, n, Pk_s are public while s_s is kept secret.

Private key generation: User **U** chooses a random number k_u, computes $K_u = H_1(ID_u,k_u)P$, and sends ID_u, K_u to **SA** over secure channel. Upon receiving the message, **SA** generates a random number r_u, calculates $R_u = K_u + r_uP$ as a witness for user **U**, and then computes partial private key as follow $x_u = H_2(ID_u,R_u)s_s + r_u$. Then, **SA** returns R_u,x_u to user **U**, who obtains his secret key as follows: $s_u = x_u + H_1(ID_u,k_u)$.

Public key extraction: Based on the pre-deployment, everyone who receives the witness R_u can compute the corresponding public key Pk_u as follows: $Pk_u = H_2(ID_u,R_u)Pk_s + R_u$.

Correctness: The public key can be computed correctly due to: $PK_u = s_uP = x_uP + H_1(ID_u,k_u)P = H_2(ID_u,R_u)s_sP + r_uP + H_1(ID_u,k_u)P = H_2(ID_u, R_u)Pk_s + R_u$.