Computer Standards & Interfaces 36 (2014) 403–411

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Secure pay while on move toll collection using VANET

Brijesh Kumar Chaurasia *[,1], Shekhar Verma [2]

Indian Institute of Information and Technology, Allahabad, India

ARTICLE INFO

Article history:
Received 2 January 2011
Received in revised form 26 November 2012
Accepted 17 August 2013
Available online 2 October 2013

Keywords:
Toll-tax collection
Vehicular ad hoc networks
Blinded coin

ABSTRACT

Manual toll tax collection requires vehicles to stop and pay. This results in long delays that nullify the aim of rapid transit of the toll roads. Existing pay as you drive techniques require offline payment and privacy breaching authentication process. In this paper, a VANET based privacy preserving secure pay while on move toll tax payment scheme is presented. The payment process is based on blinded coin in which the coin is obtained from the bank offline. As member of the VANET, a vehicle is a priori authenticated and makes online payment during the period it passes through the plaza.

1. Introduction

National highways comprise only 2% of the total length of the roads in the India and still cover 40% of overall road traffic. The NHAI (National Highway Authority of India) was formed under the NHAI Act, 1988 [1]. The government of India had given charge to NHAI for development, maintenance and management of national highways and corridors. Toll tax collection is an important constituent of corridor management. Toll is collected for the maintenance and development of highways/corridors. Every vehicle passing through the road pays a designated amount to the toll collector. Toll tax amount may be levied on the basis of vehicle type, usage frequency, nature of load, and distance traveled [2]. A vehicle pays by stopping at the toll plaza, giving the tax and collecting the receipt manually. Manual toll collection centers have manned toll booths with toll gates. After manual payment the toll gate is opened by the toll collectors. This process of stopping a vehicle, collecting of toll money, issuing of receipt and manual opening of the gate is a slow and cumbersome process. A manually operated toll plaza processes approximately 400 vehicles per hour. A queue buildup introduces substantial delay and traffic congestion at the toll collection center [2]. Congestion and delay at toll tax collection center defects the original aim of the toll road: customer gratification and efficient traffic flow. To reduce this delay, road preceding the plaza is divided into various lanes. Each lane has an independent manned toll booth for toll collection purposes. This reduces the delay significantly. This may however, be insufficient to mitigate the congestion and delay, a collection system that reduces the manual intervention. An initial automation was the plastic coin technique [3]. The user buys the coins beforehand that are collected at the toll plaza. This reduces the human intervention delay significantly. Other techniques include usage of credit card/smart card for toll collection [4,5]. However, all these systems require vehicles to stop and pay at the toll plaza. What is required is payment while on move. Automated toll tax collection is "unattended toll tax collection" and allows payment while driving option. In such open road toll system, collection of toll money is done electronically, through electronic toll system and enforcement system [2]. An electronic transaction is done between the vehicles passing through a toll plaza and toll collector. In this type of toll collection, there is no need for vehicle to slow down or stop for toll tax payment. These open road toll tax collection systems are likely to increase the speed of processing per vehicle three-fold as compared to manual toll tax collection systems [6]. However, lack of manual intervention requires security mechanisms like mutual authentication of the vehicle and the toll collector; and privacy preservation of the vehicle. In a VANET, vehicles form an ad-hoc network with the aid of road side units (RSUs) to exchange messages directly (V2V communication) or through the RSUs [7,8]. Direct V2V communication allows fast exchange of messages, both critical and non-critical [8–10]. For critical safety applications [10,11] warning messages like lane changing and intersection collision warnings are broadcast by the vehicle. Non-safety messages are related to passenger comfort and efficiency of the transportation system. The generation of these messages requires the integration of in-vehicle networking system into the VANET communication system [12].

* Corresponding author at: 102-Research Scholar Apartment, Deoghat, Jhalwa, Indian Institute of Information and Technology, Allahabad (U.P.) 211012, India. Tel.: +91 9453701376, +91 5102361501; fax: +91 532 2922100.
E-mail addresses: bkchaurasia.itm@gmail.com (B.K. Chaurasia), sverma@iiita.ac.in (S. Verma).
[1] Permanent address: 503/7C, New Rai Ganj, Near Sipri Thana, Sipri Bazar, Jhansi (U.P.) 284003, India.
[2] Tel.: +91 9450965336; fax: +91 532 2922100.

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.08.011

The present work is a VANET based variant of open road toll tax collection system in which the paying vehicle and the toll plaza are a part of the VANET. This pay while on move is free from human intervention thereby increasing the efficiency of the payment process and assumes that the member vehicles in the VANET are authenticated and do not require authentication at the toll plaza [13]. Specifically, the work addresses the issue of security in automated pay while on move toll payment. A security mechanism using blinded coin that ensures authentication, privacy preservation and genuineness of the payment is proposed. The time lightweight coin mechanism ensures that delay is small enough to allow pay while on move toll collection.

The rest of the paper is organized as follows. Section 2 describes the problem. In Section 3, related work in open road toll collection is described. The proposed secure technique for toll collection is described in Section 4. The method is evaluated through simulation and results are given in Section 5. Section 6 concludes the work.

2. Problem description

Manual toll tax collection introduces delay that nullifies the aim providing well maintained roads that reduce the overall journey time on the toll road. This delay can be avoided by collecting toll tax as electronic payment over the wireless channel. However, the lack of physical contact and the broadcast nature of wireless communication give rise to security challenges like authentication, confidentiality and privacy. The existing secured e-payment systems like SET and debit card model consume time which is usually greater than the stay time of a vehicle in the communication range of a toll plaza. The problem in the implementation of e-payment in VANET is the limited communication range of an RSU (~1000 m) and vehicles (~300 m) and speed of the vehicles (~80–100 km h^{-1}) on a highway. A speeding vehicle is in the communication range of toll bridge for a short period of time and density of nodes in vehicular environment may be very high. Vehicles have to complete the toll payment within a limited time over a contention based broadcast medium. For this, the number of steps in the transaction process and message sizes should be as low as possible to minimize the communication and processing delay overheads. Thus, the main challenge of open road toll tax collection is to device a secure light weight payment technique for low value money transfer in a high mobility, high vehicular density environment.

3. Related work

Blinded digital coin based technique [14] is employed to preserve the user privacy. Digital coin based technique requires three parties, two parties that are involved in transaction and a bank. In addition to these three parties, one more entity, the trusted third party, is also added for making the scheme completely offline. The trustee has the ability to find the cheater. The digital cash based system [15] has three basic protocol phases for payment withdrawal phase, payment phase and deposit phase. In such payment systems four parties are involved: bank, vehicle owner and toll collector with trusted third party. This blinded coin technique ensures an anonymous and unlinkable transaction of digital money among the parties. It uses a RSA based blind digital signature scheme for making the transactions anonymous. In this digital blind signature scheme, there are three parties, viz. vehicle, toll tax center and the bank. In contrast to the basic coin technique [15] in anonymous coin based technique [14], coin serial number is generated by the vehicle and then blinded by a random number used by the vehicle itself. This coin is then forwarded to the bank for blind digital signature of the coin. After the bank signature, the coin is returned back to the vehicle. The vehicle unblinds the coin and uses it for anonymous payment. When a coin is received by the toll tax center, it immediately contacts the bank to ascertain its freshness. The unforgeable nature of the blind signature ensures the security of such cash and neither the bank nor the toll tax center is able to link the vehicle identity [16,17]. The scheme is also able to avoid duplicate usage. In [18], the problem of misbehaving vehicles that pass through without paying toll is addressed. The system assumes the presence of an RFID based smart card for identification, authentication and verification of payment. The toll booth identifies the vehicle through the RFID tag, initiates the payment process and issues a certificate to the vehicle. The barrier is lifted upon successful completion of the process. A vehicle without the certificate is stopped by the physical barrier. This work, however, does not address the details of the toll collection process. In [19], the effect of electronic toll collection (ETC) on traffic congestion in the vicinity of a toll gate with both ETC and non-ETC vehicles is studied. The study assumes credit based payment with a payment delay of 4 s for an ETC vehicle and 14 s for a non-ETC vehicle. However, the payment process is not given. Other existing works [20] also address the issue of the stay time in the toll booth during the complete process involving deceleration during arrival, transaction time in payment process and exit. The 407 Express toll route (ETR) [21] is an ETC system. It is a variant of closed-access toll road in which gantries are placed at the entrance and exit points of each toll. OCR cameras are used to photograph license plate numbers of vehicles that do not have transponders. Two laser beam scanners are placed above the roadway to detect the types of vehicles passing through the gantries. The toll is calculated automatically, and a bill is sent to the registered address of the vehicle owners. There is no other way to pay 407 tolls. The process is offline and non-privacy preserving with very high infrastructure cost. VANET based toll collection is given in [22] in which the collection process is divided into association, authentication, payment and verification subprocesses. The payment framework has four entities, vehicle, RSU and two trusted authorities; bank and toll road operator. The scheme is as follows. The proposed e-toll transaction scheme is divided into three protocols. The initial e-toll purchase protocol has ten steps. In this protocol driver first registers with the register manager (trusted authority) and register manager sends the identity of the vehicle and itself to the transaction manager. The vehicle purchases e-toll from bank. The bank, then, verifies the message request of vehicle and its identity from transaction manager. Finally, it issues the e-toll to the requesting vehicle. In the second step e-toll payment protocol is subdivided into e-ticket issuing protocol and e-toll payment protocol. Each of these sub-protocols has three and four steps respectively. The problem with the scheme is the large number of message transfers for in situ procurement of the e-toll and the final online verification of the payment. In a system with large number of vehicles, these two processes may induce a delay larger than the maximum stay time of a vehicle. This makes the proposed technique unscalable and unsuitable for full fledged deployment.

4. Proposed technique — open road tax collection

The proposed technique is based on blinded coin technique given in [23]. The proposed VANET based secure toll tax payment is divided into three phases; withdrawal, payment and deposit. The first phase is the offline withdrawal phase in which the vehicle buys coins from the bank under the presumption that the tax amounts are small. A coin consists of the money designation, vehicle identity and timestamp. The bank signs the coin with a blind Schnorr signature to ascertain the privacy of the buyer. Non-repudiation of payment/non-payment is ensured by ECC based Schnorr signature by the vehicle owner. A priori purchase also ensures anonymity of the vehicle owner during the payment process. After withdrawal, vehicles have valid coins which can be used to pay the toll tax through VANET communication. The other two phases of the scheme are online phases which take place during the toll collection phase. The payment phase starts when a vehicle comes in the vicinity of a toll plaza and prepares for a payment. There are five steps in the payment phase during which a vehicle associates itself with the toll collector RSU, the vehicle and toll collector RSU mutually authenticates each other, the designated toll money is transferred from the vehicle to the RSU and a receipt is issued to the vehicle. The