Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Time-based low emission zones preserving drivers' privacy

Roger Jardí-Cedó[a], Macià Mut-Puigserver[b], M. Magdalena Payeras-Capellà[b], Jordi Castellà-Roca[a], Alexandre Viejo[a],*

[a] Departament d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Av. Països Catalans 26, E-43007 Tarragona, Spain

[b] Dpt. de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Ctra. de Valldemossa, km 7.5. E-07122 Palma de Mallorca, Spain

HIGHLIGHTS

- A complete state of the art on Electronic Road Pricing (ERP) systems is presented.
- A new ERP system that improves fraud control and drivers' privacy is proposed.
- The feasibility of the practical deployment of the system is empirically studied.

ARTICLE INFO

Article history:
Received 12 August 2015
Received in revised form
17 May 2016
Accepted 17 June 2016
Available online xxxx

Keywords:
Electronic road pricing
Privacy
Security
Low emission zone

ABSTRACT

Nowadays, big cities try to fight high levels of pollution and traffic jams by limiting the access of vehicles to centric zones or Low-Emission Zones (LEZ). One of the most important drawbacks of LEZs is the citizens' risk to be tracked by means of their interactions with the Electronic Road Pricing (ERP) system in use; another relevant problem is the significant error percentage on the detection of fraudulent drivers. The former shortcoming clearly affects the peace of mind of users regarding their privacy. The latter represents an important disadvantage for any entity willing to employ resources on managing a LEZ. In this article, a new ERP system specifically designed for cities with Low-Emission Zones is proposed. The new scheme is user-centric by design, in the sense that preserving the privacy of honest drivers is a fundamental objective. Regarding fraudulent drivers, the proposed system is able to detect them and revoke their anonymity.

1. Introduction

Circulation problems frequently take place in large metropolitan areas such as Paris, Barcelona or Rome, together with traffic jams and pollution problems, due to the huge vehicle concentration in some areas of those cities. The air quality guidelines presented by *WHO*[1] in 2013 serve as a guide on the way to reduce air pollution effects on health. Different European directives, such as 2008/50/CE, follow these recommendations to limit the level of certain environmental pollutants. The different administrations are adopting High-Occupancy Vehicle (*HOV*) lanes [1], variable speed or vehicle circulation restrictions in central areas, among other measures, so as to meet this legislation. This last measure, known as Low-Emission Zone (*LEZ*), and adopted in many cities such as London, Singapore, Tokyo or Beijing [2–4], requires the vehicles to pay in order to circulate according to certain conditions, such as weight or emissions.

Electronic Toll Collection (*ETC*) has been used in highways, tunnels or bridges in the last decades, with the aim of expediting toll payments and reducing traffic jams. Besides, Vehicular Location-Based Services (*VLBS*) such as *GPS* and wireless communication have been developed to provide information to drivers concerning their geographic location, thus improving transportation efficiency. These *ETC* systems, considered *VLBS*, are known as Electronic Road Pricing (*ERP*), and they present some improvements such as a more flexible calculus of the fees according to the distance driven, route or time. Further, when applied in urban areas, the price of the fees could be dynamically modified according to the transit density. In this way, the rise of the price in dense areas would lead drivers to avoid them. Therefore, a better traffic

* Corresponding author.
E-mail addresses: roger.jardi@urv.cat (R. Jardí-Cedó), macia.mut@uib.es (M. Mut-Puigserver), mpayeras@uib.es (M.M. Payeras-Capellà), jordi.castella@urv.cat (J. Castellà-Roca), alexandre.viejo@urv.cat (A. Viejo).

[1] http://www.euro.who.int/__data/assets/pdf_file/0020/182432/e96762-final.pdf.

http://dx.doi.org/10.1016/j.future.2016.06.012
0167-739X/© 2016 Elsevier B.V. All rights reserved.

Please cite this article in press as: R. Jardí-Cedó, et al., Time-based low emission zones preserving drivers' privacy, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.06.012

management could be achieved by controlling the flow and density of vehicles, and as a result, traffic jams would be reduced.

1.1. State of the art

In recent years, different *ERP* systems have been proposed in the literature [5–10]. They all require the use an On-Board Unit (OBU) enabled with GPS and a system of wireless communication (i.e. using ZigBee [11]), in order to exchange with the Service Provider, *SP* (see definition in Section 2.1), information related to the vehicle location and fees to pay. In these systems, the price is determined by the vehicle path. On the one hand, in [5] and [6], the information related to the path is sent by the *OBU* to an external server, property of *SP*, who fixes prices in each billing period. On the other hand, in [7–10], fees are calculated locally by each *OBU*, and are sent to *SP* server in each pricing period. In this case, the information disclosure related to the vehicle location is minimal. In this case, the use of cryptographic proofs demonstrates whether that *OBU* has been honest in the fee calculation and aggregation.

ERP systems aim to control fraud since drivers could act maliciously in order to save money (i.e. by disconnecting or modifying *OBU* data). For this reason, mechanisms based on checkpoints, *Chps* (see definition in Section 2.1), are implemented in order to test their honesty. *Chps* are randomly located on the road and equipped with cameras that register the number plates of all the vehicles that pass by. These recordings capture vehicles at a given time and place, and serve to verify that a vehicle path has not been altered. In order to achieve this, the *SP* and the driver interact in the billing period. Detecting fraud has a certain probability and it depends on the number of *Chps*. Moreover, this approach requires that the drivers ignore the number and the location of the *Chps* in order to be successful, and this is a hard requirement to comply with.

Preserving the privacy of the drivers while allowing fraud detection represents a significant trade-off in the previous *ERP* systems. When a high fraud detection level is requested, privacy is affected, that is, *SP* is capable of rebuilding a vehicle path more precisely or even link several paths, provided that the number of *Chps* is large. Moreover, precision could improve if the *Chps* are randomly moved every so often, and vehicle paths follow a routine (i.e. going to work), yet privacy would be affected.

1.2. Contributions and structure of the document

According to the limitations linked to the trade-off between preserving the drivers' privacy and performing an effective fraud detection which have been stated in the current literature, this paper presents a new user-centric *ERP* system for *LEZ*s. The main benefit of the new scheme in comparison with the most recent literature is that preserving the privacy of honest drivers is a mandatory requirement; however, achieving this does not reduce the fraud detection ratio, and this represents an additional advantage with respect to current proposals in the literature that are directly affected by the fact that they have to decide if they use more checkpoints (and improve the fraud detection while reducing the drivers' privacy) or less checkpoints (and achieve the opposite). Both benefits are obtained by means of a new architecture and a new protocol that allow the entity in charge of the *ERP* to revoke the anonymity of fraudulent drivers.

Note that, all the systems described in Section 1.1 [5–10] penalize the privacy of vehicles, honest or not, by taking a photo of them at different places. The price they pay for circulating in this kind of systems is the loss of privacy. On the other hand, in the user-centric system proposed in this article, only dishonest drivers are photographed and they are thus affected by a loss of privacy. In this case, the *Chps*, also equipped with cameras, only register fraudulent vehicles, thus keeping honest drivers' privacy. For this reason, drivers are expected to collaborate with the system to keep their privacy. That is, if a driver wants to keep her privacy, she should then behave correctly and cooperate, otherwise she will lose it. Moreover, in the proposed system, the *OBU* of the vehicle does not register its location, plus reconciliation between driver and system in the billing period is not required, and fraud control is non-probabilistic.

Table 1
Entity Table.

Key	Name	Description
LEZ	Low Emission Zone	Zone with circulation restrictions
D	Driver	Person who drives a *V*
V	Vehicle	Means of transport, which is driven by a *D*
OBU	On Board Unit	Device installed in each *V*, which executes the protocol in a *V*
SE	Secure Element	Tamper-proof device that executes
SP	Service Provider	Manager of a LEZ
Chp	Checkpoint	Points of control deployed in the entrance/exit of a LEZ
VCA	Vehicle Certification Authority	The authority who certifies *Vs*
PA	Punishment Authority	The authority who evaluates incidences and punishes fraudulent *Vs*

The system is presented in Section 2. In Section 3, the scheme is summarized. Afterward, the scheme is divided into three main protocols, *In/Out LEZ* (Section 4), *Payment* (Section 5) and *Sanction* (Section 6) protocols. Security is evaluated in Section 7, and performance and viability are presented in Section 8. Finally, conclusions are presented in Section 9.

2. System model

This section presents a system that is modeled by describing the participating actors, the requirements to be met and the several and possibly opposite interests of the actors involved.

2.1. Actors involved

The proposal considers different actors (see Table 1 for a summary of all the entities involved). *Driver D* is the person who drives a vehicle in a *LEZ*. *Vehicle V* is the mean of transport registered by a unique *D*, who is the owner of the vehicle, yet the vehicle may be driven by several *Ds*. *V* has an identifier (the vehicle plate) that connects it to the owner. *Secure element SE* is a tamper-proof security module installed by the competent traffic authority in each *V*. It performs all the sensitive operations needed to meet the security requirements. *On-board unit OBU* is installed in each *V*. It has more computational power and storage capacity than the *SE*. This device connects the *SE* with the user and performs the least sensitive protocol operations. It is enabled with GPS. *Service Provider SP* offers an ERP service for urban areas due to a concession contract with the local public administration (i.e., City Council). This entity has the right to offer this service and is responsible for managing the system. *SP* installs checkpoints in the restricted zone. *Checkpoint Chp* aims to control the access of vehicles that enter (*Chps* of entrance) or leave (*Chps* of exit) the zone. *Chps* are considered trustworthy and it is assumed that they do not take photographs indiscriminately as long as the drivers behave honestly. *Vehicle Certification Authority VCA* provides keys and certificates to *V*s. *Punishment Authority PA* is a trusted entity composed by different sub-entities or authorities. The collaboration of a minimum set of sub-entities allows them to know and reveal the identity of the owner of the *V* in case of fraud.