Computer Networks 145 (2018) 13–26

Contents lists available at ScienceDirect

Computer Networks

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

Secure and privacy-preserving lightweight access control system for low emission zones

Carles Anglès–Tafalla[a,*], Jordi Castellà-Roca[a], Macià Mut–Puigserver[b], M. Magdalena Payeras–Capellà[b], Alexandre Viejo[a]

[a] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, CYBERCAT-Center for Cybersecurity Research of Catalonia, Av. Països Catalans 26, Tarragona E-43007, Spain
[b] Departament de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Ctra. de Valldemossa, km 7,5., Palma E-07122, Spain

ARTICLE INFO

Article history:
Received 20 March 2018
Revised 12 July 2018
Accepted 17 August 2018
Available online 20 August 2018

Keywords:
Low emission zones
Privacy by design
Smart cities
Privacy
Smartphone
Security

ABSTRACT

Low Emission Zones (LEZs) are urban areas in which the access of polluting vehicles is controlled with the objective of improving the air quality. This traffic control method has been already deployed in important cities such as London or Singapore, and several others are planning to implement them in the mid-term. While the current LEZ solutions have proven to be feasible, they have also turned out to require costly infrastructures such as expensive road side units and vehicle equipment. Moreover, their intrusive nature has raised social alarms regarding the potential violation of the drivers' privacy that their use may represent. To address these issues, this paper presents an access control system for LEZs specially designed to provide effective anti-fraud measures while preserving the privacy of the drivers who behave honestly. The new scheme is lightweight enough to be used in low-cost infrastructures. Moreover, the only equipment required at the driver's side is a common smartphone enabled with typical communication capabilities. One of the cornerstones of the proposal is its deployability in real scenarios, for this reason, the feasibility of the new technology is validated in a relevant environment and an extensive evaluation is provided.

1. Introduction

Traffic congestion along with the high levels of environment pollution have become a serious problem for any large metropolitan area all over the world. In the center of those cities, the levels of air pollution exceed, mainly due to huge vehicle concentration, some of the World Health Organization (*WHO*) thresholds [1] endangering their citizens' health. In order to tackle this serious problem, governmental and state administrations are adopting measures to promote the rational use of pollutant vehicles like High-Occupancy Vehicle (*HOV*) lanes, HOV dedicated parking places or vehicle circulation restrictions, to name a few. In the same vein, one of the most adopted measures in this scheme is the so-called Low Emission Zones (*LEZ*). The concept of LEZ, which first appeared in Sweden under the name of "environmental zone" in the late 90s, consists of an area where certain restrictions or fines are applied to their users in accordance to their vehicle emissions. Following the Swedish example, several cities in Germany, the Netherlands, the United Kingdom and north Italy have implemented this solution ever since.

Among them, one of the most cited examples in the literature is the London's congestion charge and its controversial vehicle control system [2]. The center of London has operated as a LEZ since 2003 and it currently establishes fixed toll rates, weighted by potential CO2 emissions, to the vehicles passing by. In order to identify the vehicles running inside the area, the LEZ implements a control system which is composed of a large set of cameras (approx. 300) distributed over the London downtown. Notwithstanding all these infrastructure deployment, the system only guarantees a reasonable probability of dishonest driver detection. A further shortcoming is the false positives generation owing to the accuracy of the automatic plate recognition system. The revision of such cases generates personnel and management costs of approximately 98 million pounds every year.

Another much-quoted LEZ example in the literature is the so-called Electronic Road Pricing (*ERP*) implemented in Singapore. The ERP is a toll-based access control system which restricts the entrance to Singapore's central business district. This system is composed of large infrastructures, located in every access road to the

* Corresponding author.
E-mail addresses: carles.angles@urv.cat (C. Anglès–Tafalla), jordi.castella@urv.cat (J. Castellà-Roca), macia.mut@uib.es (M. Mut–Puigserver), mpayeras@uib.es (M.M. Payeras–Capellà), alexandre.viejo@urv.cat (A. Viejo).

https://doi.org/10.1016/j.comnet.2018.08.010
1389-1286/

restricted zone, which implement all needed mechanisms to collect tolls and identify dishonest users. In order to interact with ERP validation infrastructure, the users of the system must purchase a specific transmitter device and integrate it on their vehicle. Toll fees are automatically charged when vehicles drive by an access point thanks to an ad hoc debit card used by the transmitter devices. Even though Singapore's scheme has proven to be more effective than the one deployed in London, its implementation is far most costly and it is not suited for most of cities roads due to the dimensions of the required infrastructures.

Even though these approaches have shown to be feasible on their respective environments, their implementation on a practical level has proven to be quite complex and expensive, requiring costly infrastructures. The design of secure and reliable schemes that automatize the vehicle access control process while reducing the implantation costs has become a main technological challenges concerning LEZs. In addition to that, the intrusive nature of current implemented systems have arisen important challenges to the field and have revealed the need of alternative user detection systems which are friendlier to user's privacy.

1.1. Related work

Over the last years, significant improvements in the field of Vehicle Location-Based Services (*VLBS*) have nurtured the evolution of typical Electronic Toll Collection systems (*ETC*), used in the last decades to speed up the payments when accessing toll areas, into more elaborated and flexible approaches known as *Electronic Road Pricing (ERP)*. These systems are able to calculate toll fees in a more flexible way on the basis of traveled distance or elapsed time inside the restricted area. Several ERP systems have been proposed in the literature [3–8] in recent years. In all these works, the itinerary of the vehicles is determined through the use of On-Board Units (*OBU*) in order to calculate the price of the fare according to their movements inside the restricted area. For this purpose, each vehicle's OBU is equipped with a GPS to periodically collect its geographical position, and a wireless communication system to communicate with the system's infrastructure. Even though all these approaches share some features, they can mainly be generalized in two groups according to the way they compute the information related to their traveled path. In the first group, there is the Service Provider (SP) who calculates, for each billing period, the corresponding fees to pay from the path information the vehicles' OBU provide. Works in [3] and [4] are clear examples of this approach. Conversely, in the second group there is the OBU who locally calculates the fees and sends them to the SP as a unique sum in each billing period. Proposals in [5–8] are examples of this kind of system. It should also be noted that in works using this model, minimum information about the geographic location of the vehicle is disclosed. However, the use of cryptographic evidence is needed in order to prove that the OBU has been honest during the fee calculation process.

The above-mentioned ERP systems are susceptible to some fraud strategies based on physical attacks like, for example, modifying the OBU flow of data or shutting it down. In order to ensure the drivers are not committing irregularities and the OBU is managing complete and correct data, these systems implement some mechanisms to avoid this kind of attacks by means of sporadic random spot checks. The basis of these checkpoints is to register the physical location of cars through the recording of their license plates. The recordings are proof of the real location of the vehicles at a particular time and could show whether the route of a vehicle has been altered or if the OBU has been turned off. In order to proof its honesty, the drivers should demonstrate, through different privacy-providing cryptographic mechanisms, that their data are consistent with the spot check records. It should be noted that systems implementing this approach directly depend on the location and number of spot checks for fraud detection. Namely, it can be assumed that increasing the number of spot checks and changing their location will result in fraud reduction, as more dishonest users will be identified. In the light of the conclusions drawn from [6], the aforementioned anti-fraud strategy relies on the wrong assumption that spot checks are unpredictable. Spot checks are physical infrastructures composed at least by a camera and a transmission device, which could be easy to identify and difficult to relocate. In this manner, drivers could take advantage of this flaw and deliberately avoid spot checks to cheat the system and commit fraud. Increasing the number of spot checks is usually proposed to overcome this situation and detect fraudulent users with a greater probability. Nevertheless, this measure negatively compromises the privacy of honest drivers as their location is more often registered.

In recent years, more refined privacy-by-design approaches have emerged [9,10]. More specifically, the system presented in [9] introduces a more flexible way of estimating the toll fees based on the distance traveled or the elapsed time inside the restricted area, which, unlike the spot-check based approaches, offers an non-probabilistic fraud control system that does not interfere with the privacy of honest drivers. The authors in [10] improve the former scheme to dynamically change the fee price according to the traffic density. In this manner, the price increase on dense traffic areas would motivate drivers to avoid them and choose alternative routes. Therefore, it could be assumed that a better traffic management could be achieved by controlling the flow and the density of vehicles in the different areas resulting in a reduction of traffic jams.

These two works provide an alternative approach to tackle the lack of privacy-preserving solutions in the literature; however, both proposals incur in significant run time costs due to the nature of those solutions, which perform several costly operations linked to the integrated payment procedure and the key material generation steps. Furthermore, these two schemes require an ad-hoc OBU and permissions to access its functionalities. The fact that the integration of OBUs in current vehicles is not widespread, and that most of their functionalities are restricted for third-party applications, represent two significant shortcomings for those methods that undoubtedly limit their effective deployability in a near future.

1.2. Contribution and plan of this paper

In order to address the already unsolved issues found in the current literature, in this paper we propose a new lightweight, secure and privacy-preserving ERP system for delivering access control to LEZs in which the cornerstone is its deployability in real scenarios. A preliminary version of the work done was presented in our conference paper [11]. In the present work, new anti-fraud mechanisms to cover unconsidered security attacks are incorporated, including the extension of the protocol in order to reflect such countermeasures. Security and privacy discussions are also broadened to meet the new claims. Furthermore, on the basis of the protocol implementation, an extensive evaluation of the proposal under the Technology Readiness Level 5 (TRL5) according to the European Commission [12] is presented in order to validate the new technology in a relevant environment.

More specifically, our contributions include:

- It provides a non-probabilistic fraud control system that preserves the privacy of the drivers that behave honestly, while punish those who misbehave.
- It is faster than other approaches in the literature, which makes the scheme lightweight enough to be used in single-board computers and, hence, work with low cost infrastructures.