Sistema de telepeaje en zonas urbanas

Roger Jardí-Cedó *, Macià Mut-Puigserver †, M. Magdalena Payeras-Capellà †,
Jordi Castellà-Roca *, Alexandre Viejo *
* Dpt. d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Av. Països Catalans 26, E-43007 Tarragona, Spain Email: {roger.jardi,jordi.castella,alexandre.viejo}@urv.cat
† Dpt. de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Ctra. de Valldemossa, km 7,5. E-07122 Palma de Mallorca, Spain Email: {macia.mut, mpayeras}@uib.es

***Resumen*—Las Low Emission Zones (LEZ) limitan el acceso de vehículos a las zonas más céntricas de las ciudades con el objetivo de reducir la densidad del tráfico y la contaminación ambiental. Estos sistemas tienen problemas de privacidad de los conductores y de efectividad en la detección del fraude. Este artículo presenta un sistema de telepeaje para LEZ que mejora estos problemas.**

I. Introducción

Ciudades como París, Barcelona o Roma tienen problemas de circulación, con grandes atascos, y problemas de contaminación debidos a la gran concentración de vehículos en ciertas zonas. Las directrices sobre calidad del aire elaboradas por la OMS en 2005 orientan "sobre la manera de reducir los efectos de la contaminación del aire en la salud". Basadas en estas recomendaciones, diferentes directivas europeas, como la 2008/50/CE, limitan el nivel de ciertos contaminantes ambientales. Para cumplir esta legislación, las diferentes administraciones están implantando, entre otras medidas, carriles de alta ocupación [1], velocidad variable o restricciones de circulación en zonas céntricas. Esta última medida, conocida como **Low-Emission Zone (*LEZ*)** y adoptada en varias ciudades[1], establece que los vehículos paguen por circular en función de ciertas condiciones, como su peso o emisiones.

Desde hace décadas, el telepeaje electrónico o Electronic Toll Collenction (ETC) ha sido utilizado en autopistas, túneles o puentes para agilizar el pago en los peajes, y a su vez, reducir los atascos. Por otro lado, gracias a nuevas tecnologías como el GPS y la comunicación inalámbrica, se han desarrollado los vehicular location-based services (VLBS), que tienen el propósito de proporcionar información a los conductores en función de su ubicación geográfica y mejorar la eficiencia del transporte. Los sistemas ETC, entendidos como VLBS, son conocidos como **Electronic Road Pricing (ERP)** y presentan varias mejoras como un cálculo más flexible de las tasas dependiendo de la distancia recorrida, la ruta o el tiempo. Además, estos sistemas, aplicados a zonas urbanas, permiten la gestión del tráfico en zonas céntricas mediante el control del flujo y la densidad de los vehículos, reduciendo así atascos. Esto se consigue modificando el precio de las tasas de forma dinámica (el aumento del precio de las zonas más densas sugiere a los conductores evitarlas). No obstante, como se verá, estos sistemas tienen ciertos problemas de privacidad.

A. Estado del arte

En los últimos años se han propuestos, en la literatura, varios sistemas *ERP* ([2], [3], [4], [5], [6], [7]). Todos ellos requieren el uso de una On-Board Unit (OBU) con GPS y un sistema de comunicación inalámbrica con el fin de recoger y enviar al proveedor del servicio *SP* (ver definición en II-A) información relacionada con la localización del vehículo y las tasas a pagar. Es decir, la tarificación es en función de la ruta del vehículo. En [2] y [3], la *OBU* envía información del camino recorrido a un servidor externo, propiedad del *SP*, el cual tarifica de acuerdo a su trayectoria en cada periodo de facturación. En [4], [5], [6], [7], las tasas son calculadas localmente en cada *OBU* y son enviadas al servidor del *SP* en cada periodo de tarificación. En este caso, la revelación de información relacionada con la localización del vehículo es mínima. Para conseguirlo, se basan en el uso de pruebas criptográficas para demostrar que la *OBU* ha sido honesta en el cálculo y la agregación de las tasas.

El control del fraude es un objetivo importante de los sistemas *ERP*. Los conductores, para ahorrar dinero, podrían actuar de forma malintencionada (p.ej. desconectando o modificando datos de la *OBU*). Por este motivo, se implementan mecanismos basados en puntos de control *Chp*s con la intención de poner a prueba su honestedad. Los *Chp*s, situados aleatoriamente en la carretera y equipados con cámaras, registran las matrículas de todos los vehículos que los atraviesan. Estas fotos son pruebas que sitúan a un vehículo en un determinado momento y lugar, y son utilizadas para verificar que la trayectoria de un vehículo no ha sido alterada. Para ello, en el periodo de facturación el *SP* y conductor interaccionan. La detección del fraude tiene una cierta probabilidad y depende de la cantidad de *Chp*s. Además, el desconocimiento del número y de su localización, por parte de los conductores, es básico.

El nivel de privacidad de los conductores y de detección del fraude son un compromiso. Si se desea un grado de detección elevado, la privacidad se ve afectada. Es decir, el *SP* será capaz de reconstruir la trayectoria de un vehículo con más precisión si la cantidad de *Chp*s es mayor. Además, si los *Chp*s son movidos aleatóriamente cada cierto tiempo y los trayectos de los vehículos siguen una rutina (p.ej. ir al trabajo), la precisión podría ser aún mayor pero la privacidad se vería afectada.

B. Contribuciones y estructura del documento

Este artículo propone un sistema *ERP* para *LEZ*s con el objetivo de mejorar el control del fraude y la privacidad de los conductores honestos mediante anonimidad revocable. A diferencia de los otros sistemas, los *Chp*s, equipados con cámaras, registran únicamente los vehículos fraudulentos, manteniendo así la privacidad de los conductores honestos. Además, la

[1] http://lowemissionzones.eu/

OBU del vehículo no registra su ubicación, no se requiere de reconciliación entre conductor y sistema en la fase de facturación, y el control del fraude es no probabilístico.

Estructura: En la Sec. II se presenta el sistema. En la Sec. III se introduce el protocolo. En la Sec. IV se evalúa la seguridad, y en la Sec. V se presenta las conclusiones.

II. Modelo del sistema

A. Participantes involucrados

- *Conductor D:* Conduce un vehículo por una *LEZ*.
- *Vehículo V:* Está registrado con un único *D* aunque puede ser conducido por varios *D*s. *V* tiene un identificador (la matrícula) que lo enlaza con el propietario.
- *Secure element SE*: Módulo de seguridad a prueba de manipulaciones, instalado en cada *V* por la autoridad de tráfico competente. Realiza operaciones sensibles para garantizar los requisitos de seguridad del sistema.
- *On-board unit OBU:* Dispositivo de capacidad de computación y almacenamiento superior al *SE* instalado en cada *V*. Conecta el *SE* con el exterior y realiza las operaciones menos sensibles del protocolo. Dispone de un módulo de localización (GPS).
- *Service Provider SP:* Ofrece un servicio de cobro electrónico de peajes (*ERP*) para zonas urbanas gracias a una concesión pública de la administración local (p.ej. un ayuntamiento). Esta entidad, a parte de tener el derecho de ofrecer este servicio, tiene la responsabilidad de gestionar el sistema.
- *Checkpoint Chp:* Está instalado en la zona restringida por el *SP* y tiene como objetivo controlar el acceso de los *V*s que entran/salen de la zona para evitar el fraude.
- *Vehicle certification authority VCA:* Proporciona claves y certificados a los *Vs*.
- *Punisher authority PA:* Entidad de confianza que conoce la identidad del propietario del *V* y la revela si hay fraude.

B. Requisitos

A continuación se describen los requisitos del sistema, relacionados con el fraude, la privacidad, la autenticidad y la tecnología, para establecer las bases del sistema.

1) Requisitos anti-fraude: Cuando un *V* entra o sale de una *LEZ* a través de un *Chp*, ambos obtienen una **prueba de entrada** γ_i o **prueba de salida** γ_o. Esta γ_i es información que demuestra que un determinado *V* entró a la *LEZ* por un determinado *Chp* a una determinada hora. Esta *prueba* se considera **válida** si no puede ser modificada o alterada sin ser detectado una vez generada (íntegra), si sus emisores pueden demostrar que es suya (auténtica) y tampoco pueden negar su autoría (no-repudiable). Cada prueba esta **vinculada** a un *V* y un *Chp*. La **vinculación** de una prueba con un *V* garantiza que el token no puede ser usado por otro *V'* de forma voluntaria o involuntaria. Esto evita la *duplicidad* de una misma prueba cuando es utilizada por más de un *V* al mismo tiempo.

El *SP* trabaja para asegurar que todos los *D*s paguen correctamente. En caso de no ser así, el *SP* identifica a los *D*s infractores y genera evidencias que lo demuestran. El **fraude** es cometido por un *D* cuando éste conduce por una *LEZ* sin ninguna γ_i, con una γ_i no válida, con una γ_i válida de otro *V*, o si en la salida no realiza el pago correctamente. Un *SP* tampoco puede **acusar falsamente** de fraude a un *D* honesto (*D* no debe estar indefenso). Una falsa acusación ocurre cuando un *SP* afirma injustamente que un *V* no tiene una γ_i, que tiene una prueba no válida, una prueba válida que pertenece a otro *V*, o si en la salida no realiza el pago correctamente.

2) Requisitos de autenticidad: En la entrada y la salida de la *LEZ*, *V*s y *Chp*s intercambian información. Al establecer la comunicación, ambas partes, tanto *V* como *Chp*, deben demostrar su identidad a la otra parte. De esta forma, cada una puede estar segura de que la comunicación se realiza con la entidad que dice ser. En caso de no ser así, se deben tomar medidas para denunciar este hecho.

3) Requisitos de privacidad: El control del fraude por parte del *SP* puede llegar a comprometer la privacidad de los *D*s. En este caso, la curiosidad del *SP* puede causar una excesiva monitorización del sistema e incluso ser consciente de cada recorrido que hace un *V*. Con el fin de evitar un excesivo control por parte del *SP* sobre los *V*s, el sistema debe (i) garantizar la privacidad (la identidad de *D* o *V* no puede ser enlazada con ningún recorrido de ningún *V*); (ii) evitar la trazabilidad (*SP* no debe conozer el recorrido de un *V*); y (iii) proveer al *D* de un anonimato revocable (si un *D* realiza fraude, el *SP* necesita su identidad para poder sancionarlo, sólo entonces, es revelada).

4) Requisitos funcionales: La *tecnología para comunicar V*s y *Chp*s entre ellos debe permitir, a estos últimos, comunicarse con el *V* más cercano a ellos. Esto se podría conseguir combinando tecnologías de comunicación de corta/media distancia, tales cómo Wimax, ZigBee IEEE 802.15.4 o Bluetooth IEEE 802.15.1, con el uso de antenas direccionales o por triangulación, por ejemplo. La *comunicación* y el *cálculo* requerido en el protocolo deberán ser lo suficientemente rápidos para permitir una intercomunicación en movimiento entre *V*s y *Chp*s. Cualquier *interacción* con el *D* deberá ser ágil y fácil. El *sistema de pago electrónico* requerido en el sistema deberá ser anónimo y no trazeable. Además, deberá ser lo suficientemente rápido para dar tiempo a realizar la transacción en el proceso de salida de la zona más externa de la *LEZ*.

C. Modelo de los adversarios

Los intereses de *D*s y *SP* pueden ser opuestos. Por un lado, los *D*s quieren ahorrar dinero, a veces de forma deshonesta y actuando en contra del sistema. Por otro lado, el *SP* puede llegar a comprometer la privacidad de los *D*s, ya que conocer la identidad de los *V*s, en caso de fraude, le puede ser útil. Además, el *SP*, con el deseo de ganar más dinero, puede actuar deshonestamente contra los *V* acusandolos de fraude de manera infundada. Por consiguient, el control del fraude y la protección de la privacidad pueden llegar a ser objetivos opuestos.

III. Descripción del protocolo

Antes de iniciar el sistema, las entidades del sistema son inicializadas (III-A: Setup y III-B: Certificación). Además, el *SP* fija los precios de la *LEZ* (III-D: Generación de precios), por unidad de tiempo y categoría de emisiones, enviando una lista de precios, firmada por la entidad competente, a cada *Chp*.

El *SP*, cada vez que decida actualizar los precios, repetirá estas mismas operaciones.

El *SE* genera unas credenciales diferentes para *V* cada vez que entra a una *LEZ* (III-C: Generación de los certificados) para poder autenticarse correctamente con los *Chp*s que gestionan las entradas y salidas de la *LEZ*.

Cuando un vehículo *V* entra a una *LEZ* (III-E: Entrada al sistema) se comunica con un *Chp* y se autentican mutuamente. Si la autenticación con *V* falla, únicamente en esta situación, el *Chp* toma una fotografía de la matrícula del *V* como evidencia de la infracción y con ella, genera una prueba de incidencia de entrada ζ_i. La ζ_i es enviada al *PA* para verificar la existencia de fraude y proceder con la sanción. Si la autenticación es correcta, el *V* obtiene una prueba de entrada γ_i que contiene el tiempo de entrada.

Cuando un *V* sale de la *LEZ* (III-F: Salida del sistema) se comunica con un *Chp* y se autentican mutuamente. Si la autenticación con *V* es correcta, el *Chp* informa al *V* del tiempo de salida y de la cuenta destino para realizar el pago. Con dicha información, *V* calcula el importe a pagar por el tiempo de estancia y categoría de emisiones, y realiza una transacción mediante un sistema de pago electrónico. La referencia de la transacción es enviada al *Chp* como prueba del pago. Finalmente, *V* recibe una prueba de salida γ_o como recibo. Si la autenticación falla, el *Chp* toma una fotografía de *V* que forma parte de una prueba de incidencia de salida ζ_o, y la envía a *PA*.

La verificación del pago se realiza por el *SP* (III-G: Verificación del pago) a posteriori y cada cierto tiempo. Por cada pareja γ_i y γ_o asociada a un mismo *V*, el *SP* comprueba si el valor de la transacción coincide con la tarificación dependiendo del tiempo de estancia y la categoría de emisiones. Si no es correcto, genera una prueba de incidencia de pago ζ_p con estos registros y la envía a *PA*.

Cuando *PA* recibe una ζ (III-H: Sanción), la verifica. Si hay fraude, *PA* revela la identidad del propietario del *V* (revoca el anonimato) y le solicita pruebas que desmientan la acusación por parte de *SP*. En función de éstas, *PA* sanciona o no al propietario.

A. Setup

El proceso de setup es el siguiente:

1) *PA* obtiene de las autoridades competentes (p.ej. Policía):
   - Una pareja de claves asimétricas (Pk_{PA},Sk_{PA}) y un certificado de clave pública $cert_{PA}$
   - Un repositorio de certificados de las autoridades.
2) *SP* y *VCA* obtienen de las autoridades competentes (p.ej. Ayuntamiento y DGT):
   - Una pareja de claves (Pk_{SP},Sk_{SP}) y (Pk_{VCA},Sk_{VCA}), y un certificado de CA ($cert_{SP}$ y $cert_{VCA}$) emitido por las autoridades.
   - Un repositorio de certificados de las autoridades.

   La longitud de la cadena de certificación de *VCA* es 1, y 0 en el caso de *SP*. La duración de $cert_{SP}$ puede coincidir con el tiempo de concesión del servicio, sin excederlo.
3) *VCA*:
   i. Define un conjunto de vehículos $V = \{v_1, v_2, ..., v_{n_V}\}$, donde $n_V = |V|$ es la cantidad de vehículos.
   ii. Define una colección de subconjuntos $K = \{C_1, C_2, ..., C_{n_K}\}$ partición de *V*, dónde $n_K = |K|$, con $|C_i| = n_C$, $\forall i$
   iii. Genera y asocia una entidad de certificación VCA_{C_i} a cada elemento de la colección *K* ($C_1, ..., C_{n_K}$):
      iii.i. Una pareja de claves ($Pk_{VCA_{C_i}}$, $Sk_{VCA_{C_i}}$), $\forall i \in \{1, ..., n_K\}$
      iii.ii. Un certificado de CA $cert_{VCA_{C_i}}$, $\forall i \in \{1, ..., n_K\}$, con una duración c_{exp} y una longitud de la cadena de certificación de 0.
4) Cada *Chp* realiza las siguientes operaciones:
   i. Obtiene un repositorio de certificados de las autoridades y entidades (excepto de los vehículos).
   ii. Genera una pareja de claves (Pk_{Chp},Sk_{Chp})
   iii. Obtiene de *SP* un certificado de clave pública $cert_{Chp}$, conteniendo una extensión $cert_{Chp}.loc$ con sus coordenadas de localización, de manera segura.

B. Certificación

Se asume que el *SE* de cada *V* ha sido inicializado previamente con un repositorio de certificados de las autoridades de certificación, con un identificador del vehículo V_{id} y con sus especificaciones técnicas (marca, modelo, número de chasis, matricula, emisiones de CO_2 y gases contaminantes, etc.).

El proceso de certificación de un *V* es realizado por *VCA*, al comprar el vehículo y/o al pasar la Inspección Técnica de Vehículos (ITV):

1) Registra el *V* a un elemento del subconjunto *K* (a un C_i)
2) Descarga, en el *SE* del *V*, la entidad de certificación VCA_{C_i} asociada al C_i (consistente en $Pk_{VCA_{C_i}}$, $Sk_{VCA_{C_i}}$ y $cert_{VCA_{C_i}}$), mediante un canal de comunicación seguro.

C. Generación de certificados

Esta fase se realiza cada vez antes de que un *V* entre a una *LEZ*. Gracias a la entidad de certificación VCA_{C_i} instalada en el *SE* del *V* en la fase anterior, éste les permite realizar las siguientes operaciones para generar nuevos certificados de clave pública:

1) Calcula una nueva pareja de claves (Pk_{V_q}, Sk_{V_q})
2) Genera un certificado de clave pública $cert_{V_q}$ con las siguientes características:
   - Con una extensión $cert_{V_q}.idS$ que contiene el cifrado probabilístico (p.ej. usando OAEP padding [8], estandarizado en PKCS #1v2 y RFC 2437) del identificador del vehículo V_{id} con la clave pública de *PA*: $Enc_{Pk_{VCA}}(V_{id})$
   - Con una extensión $cert_{V_q}.emis$ que contiene la categoría de emisiones de CO_2 del vehículo.

D. Generación de precios

Cada vez que el *SP* modifica los precios de tarificación de una *LEZ* realiza los siguientes pasos:

1) Fija los *precios* por unidad de tiempo y categoría de emisiones (p.ej. european emission standards).
2) Genera un timestamp *ts*

3) Compone una información de precios $\theta = (precios, ts)$
4) Firma el θ: $Sign_{SP}(\theta) = \bar{\theta}$
5) Envía θ^*=(θ, $\bar{\theta}$) a cada *Chp*

E. Entrada al sistema

Cuando un *Chp* situado en la entrada de una *LEZ* detecta un *V*, se inicia el siguiente protocolo:

1) *Chp*:
   i. Genera un nonce N_A
   ii. Compone una información de entrada $\psi = (N_A, \theta^*)$
   iii. Firma el ψ: $Sign_{Chp}(\psi) = \bar{\psi}$
   iv. Envía ψ, $\bar{\psi}$ y su $cert_{Chp}$ a *V*
2) El *SE* del *V* con la ayuda de su *OBU*:
   i. Verifica el certificado $cert_{Chp}$ y la firma $\bar{\psi}$: $Verif_{Chp}(N_A,\theta^*,\bar{\psi})$
   ii. Verifica la firma $\bar{\theta}$: $Verif_{SP}(precios,ts,\bar{\theta})$
   iii. Verifica las coordenadas de localización $cert_{Chp}.loc$ del *Chp* (incluido en su certificado).
   iv. Genera un nonce N_B y calcula el fingerprint $fing_{Chp}$ de $cert_{Chp}$ (se calcula con la función hash del certificado y sirve de identificador).
   v. Compone un mensaje $\omega_{V_q} = (\theta^*, N_A, N_B, fing_{Chp})$
   vi. Firma ω_{V_q}: $Sign_{V_q}(\omega_{V_q}) = \omega\bar{}_{V_q}$
   vii. Envía N_B, $\omega\bar{}_{V_q}$ y $cert_{V_q}$ a *Chp*
3) *Chp*:
   i. Genera un timestamp ts'
   ii. Verifica el certificado $cert_{V_q}$ y la firma $\omega\bar{}_{V_q}$: $Verif_{V_q}(\theta^*, N_A, N_B, fing_{Chp}, \omega\bar{}_{V_q})$
4) Si alguna de las verificaciones falla, el *Chp* realiza:
   i. Genera un numero de incidencia de entrada in_i
   ii. Toma una fotografía *ph* de la matrícula de *V*
   iii. Procesa la matricula mat
   iv. Compone una prueba de incidencia de entrada ζ_i= (in_o,mat,*ph*,ts',θ^*,N_A,N_B,$fing_{Chp}$,$\omega\bar{}_{V_q}$,$cert_{V_q}$)
   v. Firma ζ_i: $Sign_{Chp}(\zeta_i) = \bar{\zeta}_i$
   vi. Envía $\zeta_i{}^*$=($\zeta_i, \bar{\zeta}_i$) y su $cert_{Chp}$ a *SP*
5) Si las verificaciones realizadas en 3) son correctas entonces,
   i. El *Chp*:
      i.i Calcula el $fing_{V_q}$ de $cert_{V_q}$
      i.ii Compone una prueba de entrada γ_i = (θ^*,N_A,N_B,$fing_{Chp}$,$\omega\bar{}_{V_q}$,$fing_{V_q}$,ts')
      i.iii Firma γ_i: $Sign_{Chp}(\gamma_i) = \bar{\gamma}_i$
      i.iv Envía ts' y $\bar{\gamma}_i$ a *V*
   ii. El *SE* del *V* con la ayuda de la *OBU*:
      ii.i Verifica la firma $\bar{\gamma}_i$: $Verif_{Chp}(\theta^*,N_A, N_B,fing_{Chp}, \omega\bar{}_{V_q}, fing_{V_q}, ts', \bar{\gamma}_i)$
      ii.ii Verifica ts' sea reciente:$|ts'$-*current time*$| < \delta$, donde δ es tiempo fijado
      ii.iii Guarda γ_i^* = (γ_i,$\bar{\gamma}_i$)

F. Salida del sistema

Cuando un *Chp* situado en la salida de una *LEZ* detecta un *V*, se inicia el siguiente protocolo:

1) *Chp*:
   i. Genera un timestamp ts'' y un nonce N_C
   ii. Compone un información de pago ρ = (ts'',N_C,acc), donde acc identifica la cuenta destino, del sistema de pago electrónico asumido, de *SP*
   iii. Firma el ρ: $Sign_{Chp}(\rho) = \bar{\rho}$
   iv. Envía ρ, $\bar{\rho}$ y su $cert_{Chp}$ a *V*
2) El *SE* del *V* con la ayuda de su *OBU*:
   i. Verifica el certificado $cert_{Chp}$ y la firma $\bar{\rho}$: $Verif_{Chp}(ts'', N_C, acc, \bar{\rho})$
   ii. Verifica las coordenadas de localización $cert_{Chp}.loc$ del *Chp* (incluido en su certificado).
   iii. Verifica ts'' sea reciente: $|ts''-$*current time*$| < \delta$
   iv. Recupera el ts' del último registro γ_i
   v. Calcula el tiempo de estancia τ a LEZ: (ts''-ts')=τ
   vi. Recupera los *precios* contenido en el θ^* del γ_i
   vii. Calcula y acumula en *amount* la cantidad de dinero a pagar en función de τ, de sus emisiones y los *precios*
   viii. Realiza una transferencia según *amount* a la cuenta destino acc y obtiene una referencia *trans*
   ix. Genera un nonce N_D y calcula el $fing_{Chp}$
   x. Compone un mensaje ω_{V_q} = (ts'', N_C, N_D, $fing_{Chp}$,*trans*)
   xi. Firma ω_{V_q}: $Sign_{V_q}(\omega_{V_q}) = \omega\bar{}_{V_q}$
   xii. Envía N_D, *trans*, $\omega\bar{}_{V_q}$ y $cert_{V_q}$ a *Chp*
3) *Chp* verifica el certificado $cert_{V_q}$ y la firma $\omega\bar{}_{V_q}$: $Verif_{V_q}(ts'', N_C, N_D, fing_{Chp}, trans, \omega\bar{}_{V_q})$
4) Si alguna de las verificaciones falla, el *Chp* realiza:
   i. Genera un numero de incidencia de salida in_o
   ii. Toma una fotografía *ph* de la matrícula de *V*
   iii. Procesa la matrícula mat
   iv. Compone una prueba de incidencia de salida ζ_o=(in_o,mat,*ph*, ts'',N_C,N_D,$fing_{Chp}$,$trans$, $\omega\bar{}_{V_q}$,$cert_{V_q}$)
   v. Firma ζ_o: $Sign_{Chp}(\zeta_o) = \bar{\zeta_o}$
   vi. Envía $\zeta_o{}^*$=($\zeta_o, \bar{\zeta_o}$) y su $cert_{Chp}$ a *SP*
5) Si las verificaciones realizadas en 3) son correctas entonces,
   i. El *Chp*:
      i.i Calcula el $fing_{V_q}$ de $cert_{V_q}$
      i.ii Compone una prueba de salida γ_o = (ts'', N_C,N_D,$fing_{Chp}$,$trans$,$\omega\bar{}_{V_q}$,$fing_{V_q}$)
      i.iii Firma γ_o,$Sign_{Chp}(\gamma_o)$=$\bar{\gamma_o}$, y lo envía a *V*
   ii. El *SE* del *V*, con la ayuda de la *OBU*:
      ii.i Verifica la firma $\bar{\gamma_o}$: $Verif_{Chp}(ts''$,N_C,N_D, $fing_{Chp}$,$trans$,$\omega\bar{}_{V_q}$, $fing_{V_q}$,$\bar{\gamma_o}$)
      ii.ii Guarda γ_o^* = (γ_o,$\bar{\gamma_o}$)

G. Verificación del pago

Cada *Chp* envía periódicamente todas las γ_i, γ_o y ζs (ζ_i y ζ_o) a *SP*. *SP* reenvia ζ_i y ζ_o a *PA*. Además, el *SP* realiza las siguientes verificaciones cada cierto tiempo (en batch) por cada conjunto de registros γ_i y γ_o asociados a un mismo V_q (con un mismo $fing_{V_q}$):

1) Extrae ts', ts'', y $cert_{V_q}.emis$, contenidos en γ_i y γ_o
2) Extrae *precios*, contenido en el θ^* del γ_i
3) Extrae la referencia *trans*, contenida en γ_o
4) Calcula el tiempo en la zona τ=ts''-ts'

5) Calcula la cantidad total a pagar $amount'$ en función de τ, $cert_{V_q}.emis$ y *precios*
6) Verifica si $amount = amount'$
7) Verifica que la transferencia se haya realizado
8) Verifica que *trans* haya sido utilizado en otra γ_o (p.ej. buscando duplicados)
9) Si la verificación falla,
   i. Genera un numero de incidencia de verificación in_v
   ii. Compone una prueba de incidencia de pago ζ_p con γ_i y γ_o de V_q: ζ_p=(in_v,γ_i,γ_o). En caso que *trans* haya sido reutilizado, añade la γ'_o que lo demuestra ζ_p = (in_v, γ_i, γ_o, γ'_o)
   iii. Firma ζ_p: $Sign_{SP}(\zeta_p) = \bar{\zeta_p}$
   iv. Envía $\zeta_p{}^*$=(ζ_p,$\bar{\zeta_p}$) y su $cert_{SP}$ a *PA*

H. Sanción

PA realiza las siguientes operaciones en función del tipo de incidencia ζ recibida:

1) Si es una ζ_i o ζ_o:
   i. Verifica las firmas
   ii. Recupera la matricula mat de la foto adjuntada
2) Si es una ζ_p:
   i. Verifica todas las firmas contenidas en ζ_p y que el firmante de γ_i y γ_o sea el mismo vehículo.
   ii. Verifica el pago repitiendo los pasos 1-7 de III-G
   iii. Si se trata de un pago duplicado, se verifica que γ_o y γ'_o contengan el mismo *trans*
   iv. Si ratifica la incidencia, recupera el identificador V_{id} de V_q (en caso de pago duplicado, se realiza sobre el último *V* en salir de *LEZ*) abriendo la extensión $certV_q.idS$ (del certificado $certV_q$ contenido en el registro γ_i o γ_o): $Dec_{PA}(certV_q.idS) = V_{id}$
3) Se pone en contacto con el propietario del *V* a partir de la mat o del V_{id}, le informa del proceso sancionador y le exige pruebas que lo refuten.
4) Si el propietario presenta pruebas, se evalúan. En caso de haber fraude, se le multa en función del tipo de infracción.

IV. Análisis de seguridad/requisitos

En esta sección analizamos las propiedades de seguridad de nuestro protocolo. La discusión esta organizada en tres proposiciones que con sus respectivas reivindicaciones proporcionan evidencias del cumplimento de las propiedades de seguridad del esquema.

Proposición 1. *La propuesta preserva la autenticidad, el no repudio y la integridad de las pruebas de entrada y de salida.*

Reivindicación 1. *No es posible la creación de pruebas de entrada o salida fraudulentas.*

Prueba. Las pruebas de entrada tienen la forma siguiente γ_i = (θ^*,N_A,N_B,$fing_{Chp}$,$\omega_{\bar{V}_q}$,$fing_{V_q}$,ts'). El checkpoint firma la prueba de entrada γ_i: $Sign_{Chp}(\gamma_i) = \bar{\gamma_i}$ y envía el par ts' y $\bar{\gamma_i}$ al vehículo. Análogamente, la prueba de salida γ_o = (ts'', N_C,N_D,$fing_{Chp}$,*trans*,$\omega_{\bar{V}_q}$,$fing_{V_q}$) es firmada por el checkpoint, $Sign_{Chp}(\gamma_o)$=$\bar{\gamma_o}$,y enviada al vehículo. Por tanto la creación de pruebas de entrada y de salida falsas es computacionalmente imposible actualmente si no se dispone de la clave secreta utilizada por el *Chp* en la firma.

Reivindicación 2. *Los* Chp*s emisores de las pruebas de entrada y de salida no pueden negar las emisiones de las mismas.*

Prueba. Las pruebas de entrada son generadas y firmadas por su emisor (los *Chp*s) y, considerando que el esquema de firma es seguro, esta operación solamente la pueden realizar ellos. Por lo tanto, la identidad del Chp está asociada a la prueba de entrada o de salida y por las propiedades del esquema de firma electrónica estos no pueden negar su autoría.

Reivindicación 3. *El contenido de las pruebas de entrada y de salida no puede ser modificado por los vehículos.*

Prueba. Suponiendo que el esquema de firma es seguro y que la función resumen utilizada en la firma es resistente a colisiones, si se modifica el contenido del billete la verificación de la firma de los billetes será incorrecta dado que $Sign_e(m) = E_{Sk_e}(h(m)) = \bar{m}$. Para que la verificación fuera correcta se debería volver a generar la firma realizada sobre el resumen del nuevo contenido. Esta operación no es posible so no se dispone de la clave secreta del checkpopint.

Resultado de la Proposición 1. *De acuerdo con las pruebas presentadas en Claims 1, 2 y 3, puede asegurarse que el protocolo satisface los requerimientos de seguridad necesarios (autenticidad, integridad y no repudio) para que las pruebas puedan considerarse válidas.*

Proposición 2. *El sistema de telepeaje presentado aquí preserva la privacidad de sus usuarios manteniendo su anonimato y evitando la trazabilidad de sus acciones.*

Reivindicación 4. *El sistema garantiza el anonimato de sus usuarios honestos.*

Prueba. La información que el usuario debe transmitir para entrar al sistema es ω_{V_q} = ($N_A, N_B, fing_{cert_{Chp}}$) y su firma. El Chp comprobará la firma con el certificado $cert_{V_q}$ que acompaña el mensaje del usuario. Este certificado (generado por el SE del *V* antes de la entrada a la *LEZ*) identifica el vehículo, pero esta información está protegida con un cifrado asimétrico usando la clave pública de la PA. Por tanto, el Chp puede comprobar la firma pero no identificar al vehículo. Posteriormente, el Chp genera y transmite al usuario la $\bar{\gamma_i}$. Con esta prueba el vehículo puede entrar a la *LEZ*. La $\bar{\gamma_i}$ no tiene más información del usuario que la contenida en ω_{V_q}. Esto significa que *V* entrará a la *LEZ* sin ser identificado.

Referente a la salida del sistema y, dejando de lado el sistema de pago que pueda ser utilizado (suponemos un sistema de pago que permita el anonimato), el usuario debe enviar al Chp de salida la siguiente información: ω_{V_q} = ($ts, N_C, N_D, fing_{cert_{Chp}}$,*trans*). Al suponer que el pago es anónimo, no se puede identificar al usuario a través de *trans*. Tampoco, por la razón explicada en el anterior parágrafo se puede identificar al usuario a través de la firma de ω_{V_q}. Consecuentemente la salida y la entrada de usuarios honestos en una *LEZ* utilizando el sistema presentado aquí son anónimas.

Reivindicación 5. *EL protocolo de telepeaje no permite rastrear o enlazar las operaciones de los vehículos.*

Prueba. La información que genera la ejecución del protocolo no permite enlazar las distintas entradas y salidas de

las *LEZs* que pueda realizar un vehículo ya que el protocolo descrito en III.C se ejecuta cada vez que el *V* accede a una *LEZ*. Esto significa que el SE de vehículo genera un nuevo $cert_{V_q}$ cada nueva entrada. Este certificado es el único elemento que podría identificar al *V*. Ahora bien, teniendo en cuenta que el uso del certificado es único para cada entrada/salida, nadie puede relacionar el *V* de esta entrada/salida con otra ninguna otra entrada/salida.

La información que se podría repetir en otra entrada/salida del mismo *V* es el campo $cert_{V_q}.idS$ del certificado donde se encuentra la identidad del vehículo. Pero, tal y como se especifica en el protocolo, el $cert_{V_q}.idS$ esta calculado a partir de un cifrado probabilístico utilizando, por ejemplo, un sistema de padding OAEP que implica que el resultado de cada nueva operación de cifrado de las credenciales del *V* sea diferente.

Resultado de la Proposición 2. *El esquema de telepeaje presentado aquí preserva la privacidad de acuerdo con las argumentaciones 4 y 5: los usuarios pueden utilizar el sistema de forma anónima y cada uno de los usos no pueden ser relacionados entre si con respecto a la identidad de los vehículos.*

Proposición 3. *El sistema de telepeaje posee los requisitos antifraude en cuanto a la corrección y verificabilidad de las evidencias generadas en el protocolo.*

REIVINDICACIÓN 6.

Se puede identificar a los defraudadores gracias al sistema de revocación del anonimato que posee el protocolo.

PRUEBA. En caso que los usuarios no realicen de forma correcta la autenticación en la entrada y/o salida del sistema pueden perder el anonimato ya que el Chp realizará una foto al *V* y capturará la matricula. Esta información es enviada a la *PA* que actuará de la forma especificada en el protocolo de *Sanción*. En la ejecución del protocolo de *Sanción* la *PA* tiene la capacidad de identificar al usuario a través de la matricula del vehículo.

En caso que los usuarios no hayan realizado el pago de la forma correcta, la *SP* en el protocolo de *Verificación de pago* comprueba que la cantidad pagada se corresponda con la tarificación establecida en función de τ y de las emisiones de *V*. Si la verificación falla, se envía esta información a la *PA* para que el usuario sea sancionado. La *PA* ratifica la incidencia e identifica al usuario abriendo el campo del certificado $certV_q.idS$ con su clave secreta. La obtención de V_{id} permite identificar y sancionar la usuario deshonesto.

REIVINDICACIÓN 7.

La ejecución del protocolo genera evidencias para que un usuario honesto pueda guardar en su OBU *y pueda usarlas para comprobar o rebatir las acusaciones de fraude.*

PRUEBA. En el momento que un usuario es acusado de no realizar correctamente la autentificación se genera una pdi que registra la incidencia. El usuario puede ser acusado de usar un certificado $cert_{V_q}$ inapropiado o de realizar una firma $\omega_{\bar{V}_q}$ incorrecta. En ambos casos, durante el procedimiento de *Sanción* la *PA* se pone en contacto con él para que pueda aportar a la pruebas para rebatir la acusación.

Un usuario honesto podrá recuperar de su *OBU* un $cert_{V_q}$ que se corresponda con su vehículo (identificado por *mat*) o una $\omega_{\bar{V}_q}$ que la haya generado correctamente el *SE* con la ayuda de la *OBU* del usuario durante la el protocolo de entrada/salida de la *LEZ*. Cabe recordar que los requisitos del sistema establecen que la *OBU* de un vehículo tenga suficiente capacidad de almacenamiento para poder verificar las posibles acusaciones de fraude que se produzcan.

En caso de una incidencia de pago, el usuario debe demostrar que ha hecho el pago de acuerdo con los datos de $\bar{\rho}$ y $\bar{\gamma_o}$ (ambos firmados por el Chp). Por tanto, un usuario honesto podrá recuperar estas informaciones de su *OBU* y remitirlas a la *PA* para rebatir la acusación.

Resultado de la Proposición 3. *El esquema de telepeaje presentado controla el fraude y puede identificar a los usuarios que lo han cometido realizando la correspondiente sanción. El protocolo permite también a los usuarios honestos obtener evidencias de su buen funcionamiento para desmentir posibles sanciones que se deban a algún tipo de funcionamiento incorrecto de los actores del sistema.*

V. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se ha presentado un sistema *ERP* para áreas urbanas que proporciona un sistema de control del fraude robusto con un elevado nivel de privacidad. Se controla la entrada y la salida de la LEZ de manera que se tarifica de forma justa y anónima. No obstante, si un usuario comete fraude es identificado mediante una foto, o gracias a la revocación de su privadidad.

Como trabajo futuro se considera la extensión del protocolo para considerar más de una LEZ, y su implementación para evaluar su aplicación práctica.

AGRADECIMIENTOS

Este trabajo está parcialmente financiado por Govierno de España (a través de una beca FPI BES-2012-054780 y los proyectos CO-PRIVACY TIN2011-27076-C03-01, ARES-CONSOLIDER INGENIO 2010 CSD2007-00004 y BallotNext IPT-2012-0603-430000). Las opiniones, de los autores que pertenecen a la Cátedra UNESCO de privacidad de datos, expresadas en este artículo no reflejan necesariamente la posición de la UNESCO ni la comprometen.

BIBLIOGRAFÍA

[1] "Resolución int/2836/2013." CVE-DOGC-B-14013017-2014. Núm 6541 - 15.1.2014.
[2] A. R.A.Popa, H.Balakrishnan, "Vpriv: protecting privacy in location-based vehicular services," in *SSYM'09*, 2009.
[3] S. J. X.Chen, G.Lenzini, "A group signature based electronic toll pricing system," in *ARES'12*, 2012.
[4] C. C. B. I. J.Balasch, A.Rial, "Pretp: Privacy-preserving electronic toll pricing," in *SSYM'10*, 2010.
[5] S. H. S.Meiklejohn, K.Mowery, "The phantom tollbooth: privacy-preserving electronic toll collection in the presence of driver collusion," in *SSYM'11*, 2011.
[6] E. I. J.Day, Y.Huang, "Spectre: spot-checked private ecash tolling at roadside," in *WPES '11*, 2011.
[7] B. F.Garcia, E.R.Verheul, "Cell-based privacy-friendly roadpricing," *Comput. Math. Appl.*, 2013.
[8] M.Bellare and P.Rogaway, "Optimal asymmetric encryption–how to encrypt with rsa," 1994.