(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 298**

(21) Número de solicitud: 201200215

(51) Int. CI.:

G06Q 20/00 (2012.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

28.02.2012

(43) Fecha de publicación de la solicitud:

30.09.2013

(56) Se remite a la solicitud internacional:

PCT/ES2013/000032

(71) Solicitantes:

UNIVERSITAT ROVIRA I VIRGILI (100.0%)
C/ de l'Escorxador s/n
43003 Tarragona ES

(72) Inventor/es:

DOMINGO FERRER, Josep;
RAFOLS SALVADOR, Carla y
ARAGONÉX VILELLA, Jordi

(74) Agente/Representante:

TORNER LASALLE, Elisabet

(54) Título: **Método y sistema de cobro sin contacto, por el uso de una vía, para vehículos de alta ocupación**

(57) Resumen:

Método y sistema de cobro sin contacto, por el uso de una vía, para vehículos de alta ocupación.

Cada ocupante de un vehículo circulando por la vía posee un dispositivo de computación con capacidad de telecomunicación, identificable individualmente, y el método propone una interacción sin contacto con los dispositivos de computación desde una estación de cobro, proporcionando un importe a pagar función del número de ocupantes del vehículo, realizando la determinación del número de ocupantes por adquisición y recuento de un número total de firmas digitales parciales realizadas los ocupantes mediante una aplicación informática albergada en su dispositivo de computación que implementa un esquema de firma digital basado en la identidad, con umbral dinámico garantizando el anonimato de los ocupantes. El sistema comprende los dispositivos de computación con una aplicación informática instalada, una estación de cobro con medios para interactuar con los dispositivos y una autoridad certificadora.

ES 2 424 298 A1

DESCRIPCIÓN

Método y sistema de cobro sin contacto, por el uso de una vía, para vehículos de alta ocupación

Sector de la técnica

La presente invención hace referencia, en un primer aspecto, a un método de cobro sin contacto, por el uso de una vía, en particular una vía de peaje tal como una autopista, por la que circulan vehículos de alta ocupación.

La invención tiene como objetivo facilitar el cobro en una estación de peaje sin contacto de manera segura y personalizada, adaptando la cantidad a pagar al número de ocupantes o pasajeros del vehículo, al mismo tiempo que se garantiza la privacidad de éstos.

La invención propone dos variantes del método para el cobro sin contacto de un peaje (por el uso de una vía), una primera para el caso en el que se calcula la cuota del peaje independientemente de los puntos de entrada en la autopista (sin tiquete) y otro para el caso en el que los vehículos reciben un tiquete a la entrada de la autopista y se les cobra de acuerdo al número de kilómetros recorridos (con tiquete).

La invención concierne asimismo, en un segundo aspecto, a un sistema para implementación del método de cobro sin contacto citado.

***Antecedentes* de la invención**

La preocupación por las emisiones de dióxido de carbono está motivando nuevos esquemas de cobro de peaje con el objetivo de ofrecer tarifas más bajas para vehículos que transporten más ocupantes (vehículos de alta ocupación o VAO).

Algunas invenciones anteriores divulgan sistemas y/o métodos de pago de peajes que tratan de cumplir con las normas establecidas para el uso de carriles destinados a vehículos compartidos.

La US 2001/0137773 A1, 'Devices, Systems and methods for identifying and/or billing an individual in a vehicle' de Potts et al., propone una solución en la que cada uno de los ocupantes posee un dispositivo móvil que transmite un identificador único a algún dispositivo del vehículo que, por medio de una antena, determina según su proximidad quién es el conductor y se comunica con la cabina de peaje.

En US 2010/0106567 A1, 'System and method for electronic toll collection based on vehicle load' de McNew et al., el vehículo posee una tarjeta electrónica que transmite un identificador y el número de ocupantes en el vehículos. Dicho número es obtenido mediante el uso de distintos métodos, y la estación de peaje comprobará, posteriormente, la veracidad de los datos recibidos.

La patente US 7,091,880 B2, 'Licensed driver detection for high occupancy toll lane qualification' de Sorensen et al., sugiere que cada vehículo posea un lector de licencias de conducir. Una vez leída la licencia, los datos resultantes se cifran y se transmiten a la entidad responsable del peaje. US 7,408,480 B2, 'Dual mode electronic toll collection transponder' de Sun Yee Woo et al., propone un sistema en el que, mediante un transmisor instalado en el vehículo, datos como el número de placa, las emisiones de vehículos, etc. se transmiten de modo cifrado a un sistema externo que cargará el importe al vehículo.

La US 4,303,904 A 'Universally applicable, in-motion and automatic toll paying system using microwaves' de Chasek et al., propone el uso de un transmisor-receptor interno en el vehículo que trasmite la información necesaria para calcular el importe. JP 2000/172892 'A vehicle charge calculating system' propone el uso de dispositivos externos para determinar las emisiones del vehículo y calcular el importe a pagar.

LA US2010161392 (A1) propone, en un ejemplo de realización (ver párrafo [0028]), contar el número de ocupantes de un vehículo mediante la detección, por parte de un lector RFID implementado, por ejemplo, en un dispositivo de uno de los ocupante unas etiquetas RFID de dispositivos o elementos llevados por el resto de ocupantes.

Todas las invenciones anteriores sólo describen métodos automatizados de gestión de un sistema de peaje en un carril de transporte colectivo con diferentes dispositivos para detectar personas o las emisiones de carbono que genera el vehículo mediante el uso de dispositivos adicionales en los propios vehículos.

En la US20040049424A1 se propone un método y un sistema para promocionar el viaje compartido (ridesharing) que describe (ver párrafo [56]) determinar el número de "participantes que viajan juntos" localizando los teléfonos móviles llevados por los mismos, y realizar un cobro en función del número de ocupantes.

En la presente invención se utilizan igualmente unos dispositivos de computación autónomos con capacidades de telecomunicación, tales como un teléfono móvil inteligente (por ejemplo, un teléfono móvil de última generación o smartphone) por cada ocupante del vehículo, pero como característica relevante se garantiza la privacidad y el anonimato de los ocupantes, durante su recuento.

Exposición de la invención

La presente invención aporta para alcanzar el objetivo explicado, en un primer aspecto, un método de cobro sin contacto, por el uso de una vía, concebido para gestionar vehículos de alta ocupación, en el cual como premisa se establece que cada uno de los ocupantes de un vehículo que implementa el método de cobro ha de poseer un dispositivo de computación autónomo con capacidad de telecomunicación, identificable mediante un identificador individual Id, o dirección de red, tal como un teléfono móvil inteligente comprendiendo el método determinar el número de ocupantes de un vehículo utilizando información acerca de dichos dispositivos de computación autónomos con capacidad de telecomunicación, mediante una interacción sin contacto con los mismos desde un centro de control de la vía o estación de cobro, para proporcionar un importe del pago por el uso de la vía, en función del número de ocupantes del vehículo. Dicha interacción sin contacto utiliza una tecnología de telecomunicación conocida, escogida entre Bluetooth, Wifi, RFID, o cualquier otra, que soporten los dispositivos de computación autónomos con capacidad de telecomunicación de los ocupantes del vehículo.

A diferencia de las propuestas de los documentos del estado de la técnica referidas, el método de cobro sin contacto de esta invención propone que dicha determinación del número de ocupantes se lleve a cabo por la adquisición y recuento de un número total de firmas digitales parciales realizadas por cada uno de los ocupantes del vehículo mediante una aplicación informática albergada en su respectivo

dispositivo de computación autónomo con capacidad de telecomunicación, aplicación que implementa un esquema de firma digital basado en la identidad, con umbral dinámico, que garantiza el anonimato de dichos ocupantes del vehículo y la seguridad de la interacción centro de control (o estación de cobro/peaje)-ocupantes.

Para la implementación del método se ha previsto asimismo que cada ocupante del vehículo adquiera previamente o contemporáneamente al viaje (pero antes de realizar el pago) una cantidad a modo de crédito que le proporciona un código de pago y el pago se realiza en dicho centro de control, sin contacto, por parte de uno o más de los ocupantes, desde su dispositivo de computación autónomo con capacidad de telecomunicación, conservando el anonimato.

Por otro lado la citada interacción sin contacto centro de control-ocupantes comprende la participación de una autoridad certificadora que proporciona a cada uno de los ocupantes del vehículo un conjunto de claves públicas y claves privadas para realizar las citadas firmas digitales parciales.

En un segundo aspecto la invención propone un sistema de cobro, sin contacto, por el uso de una vía, para vehículos de alta ocupación, que integra los siguientes elementos:

- una estación para cobro de una tasa variable por el uso de la vía, con medios de telecomunicación;

- un dispositivo de computación autónomo, para cada uno de los ocupantes, con capacidad de telecomunicación (por ejemplo un teléfono móvil inteligente), con un identificador individual Id o dirección de red;

- al menos una aplicación instalable en los dispositivos de computación autónomos con capacidad de telecomunicación, para implementar el método de cobro sin contacto mediante dichos dispositivos de computación autónomos;

- una autoridad certificadora que proporciona un conjunto de claves públicas y claves privadas para realizar unas firmas digitales parciales utilizando dichos dispositivos de computación autónomos; y

- medios establecidos en un centro de control o de cobro, tal como dicha estación de cobro/peaje, para interacción bidireccional sin contacto de dicho centro de control para cobro por uso de la vía, con dichos dispositivos autónomos con capacidad de telecomunicación.

Dichos elementos están previstos para operar en combinación para implementar el método de cobro sin contacto propuesto, que comprende el recuento de dichas firmas digitales parciales de los ocupantes del vehículo.

En un ejemplo de realización del método de la presente invención la citada vía de pago es una vía de peaje de tarificación variable en función del número de ocupantes de cada vehículo que cruza el peaje, interviniendo en este escenario al menos los siguientes agentes:

- una estación para cobro de un peaje (con funciones del citado centro de control) con medios de telecomunicación;

- un dispositivo de computación autónomo, para cada uno de los ocupantes, con capacidad de telecomunicación, con un identificador individual Id o dirección de red;

- una autoridad certificadora que proporciona un conjunto de claves públicas y claves privadas para realizar dichas firmas digitales parciales; y

- al menos una aplicación instalable en los dispositivos de computación autónomos para implementar el método mediante dichos dispositivos de computación autónomos,

El método propuesto se caracteriza por las siguientes etapas:

a) autenticación ante una autoridad certificadora de cada uno de los n ocupantes del vehículo a partir de dicho identificador individual que asocia a la identidad del ocupante del vehículo un único número Id, de misma longitud;

b) generación para cada ocupante de un conjunto de L claves públicas y las correspondientes claves privadas por parte de dicha autoridad certificadora, en donde para i=1 hasta L el par i-ésimo de claves es solamente función del valor del i-ésimo dígito (o del i-ésimo grupo de dígitos) menos significativo de Id (de este modo el par i-ésimo de claves es compartido por todos aquellos ocupantes del vehículo que comparten el mismo valor para el digito/grupo de dígitos i-ésimo, con lo que al usarse dicho par de claves no se revela quién de los usuarios que lo comparten lo ha usado, lo cual proporciona un eficaz anonimato)

c) transferencia de dichas claves privadas generadas a su respectivo ocupante;

d) adquisición por cada ocupante de una cantidad a modo de crédito que proporciona un código de pago (esta adquisición se puede realizar de manera anónima o mediante una tarjeta de crédito);

e) uno de los ocupantes del vehículo Um (maestro) adopta un papel principal y cada uno de los ocupantes del vehículo establece un dígito/posición o grupo de dígitos/posiciones de cada uno de sus identificadores personales Id, que sea distinto para cada uno de dichos ocupantes, sea esta posición/grupo la j-ésima (esta etapa puede realizarse en cualquier momento de formación o consolidación de la agrupación de ocupantes del vehículo, en un momento dado);

f) la estación de peaje proporciona para cada vehículo próximo a la estación de peaje un identificador de transacción Ts con una marca de tiempo (esta etapa puede realizarse contemporáneamente ante una petición de pago o detección de un vehículo por parte de la estación de peaje);

g) cada uno de los ocupantes del vehículo realiza una firma parcial con umbral n (siendo n el número de ocupantes del vehículo) con su clave privada j-ésima del mensaje formado por Ts concatenado con las claves públicas j-ésimas de todos los ocupantes y se envían dichas firmas parciales;

h) adquisición o recepción por dicha estación de peaje de una firma final en nombre del grupo, a partir de las citadas firmas parciales;

i) verificación por parte de dicha estación de peaje de dicha firma final de grupo, cual firma solo será válida si han participado en ella n ocupantes, con lo que permite determinar de forma segura y anónima el número n de ocupantes del vehículo, y

j) aplicación por parte de la estación de peaje de un importe prestablecido conforme a unos baremos tarifarios según el número de ocupantes, y petición de dicha cantidad a los ocupantes del vehículo para habilitar un pago.

El referido envío de las firmas parciales de la etapa g) se realiza por parte de cada uno de los ocupantes a un ocupante Um, el cual combina las firmas parciales y obtiene una firma final de grupo, representativa de los n ocupantes, que es enviada a la estación de peaje, o puede realizarse alternativamente por parte de cada ocupante del vehículo a la estación de cobro de un peaje, en donde se combinan las firmas parciales y se obtiene una firma final de grupo, representativa de los ocupantes.

En general el pago será asumido por uno o más ocupantes del vehículo que se dividen el importe a pagar que es transferido de forma segura a partir de uno de los dispositivos de computación autónomos, en particular del de dicho Um.

En cuanto a la citada transferencia de dichas claves privadas de la etapa c), ésta se realiza por parte de una oficina bajo un esquema presencial o por conexión remota con la misma e identificación segura por parte de un ocupante o potencial ocupante del vehículo.

En un ejemplo de ejecución para implementar la etapa f) la estación de peaje detecta los identificadores Id de dichos dispositivos de computación autónomos con capacidad de telecomunicación de los ocupantes del vehículo, reconoce el número de dispositivos que viajan en el vehículo y les envía un identificador de transacción Ts con marca de tiempo.

En otro ejemplo de ejecución se ha previsto que la estación de peaje realice previamente a dicha etapa f) un envío de solicitud de pago al ocupante Um.

Asimismo, en el caso de pago utilizando tiquetes, una marca de tiempo Msg y un localizador de referencia de un peaje de entrada, son enviados por una estación de peaje de entrada a los ocupantes del vehículo y cada ocupante de los que va a colaborar en el pago envía dicha Msg concatenada con un código de pago y cifrado con la clave pública del peaje al ocupante Um. El ocupante Um o la estación de peaje concatena todos los mensajes cifrados recibidos de los ocupantes del vehículo que van a pagar junto con las claves públicas j-ésimas de los ocupantes, sea "Centry" el mensaje resultante de dicha concatenación, y la estación de peaje devuelve como tiquete el mensaje "Centry" recibido de los ocupantes firmado con la clave privada del peaje y el ocupante Um almacena Centry y el tiquete en su dispositivo de computación autónomo.

El método prevé asimismo como un ejemplo de ejecución que en la salida del peaje, en la etapa g) dicho ocupante Um envíe además "Centry" y el tiquete.

Finalmente el método comprueba que en el momento de realizar el pago concidan los ocupantes que se ofrecieron a pagar en la entrada del peaje con los que pagan en la salida, evitando cambios fraudulentos de tiquetes.

Descripción en detalle de la invención y de unos ejemplos de implementación

El sistema propuesto comprende:

- una aplicación en un dispositivo móvil App_U por cada ocupante U de un vehículo que:

  - permite el cálculo de firmas con Π en nombre de U, donde Π es un esquema de firma digital con umbral dinámico y basada en identidad (identity-based dynamic threshold digital signature scheme),
  - permite el cálculo de datos cifrados con Π', un esquema de cifrado de clave pública con la clave pública de la entidad de certificación pk^{CA},
  - se puede ejecutar en modo maestro o esclavo. En cada uno de estos modos App_U tiene un papel diferente en el protocolo de pago,
  - incluye un certificado que permite comprobar la validez de la clave pública pk^{CA}

- una autoridad de certificación (*CA*), por ejemplo, la empresa responsable del sistema de pago del peaje, que distribuye las aplicaciones para los dispositivos móviles, junto con las claves secretas necesarias después de la etapa de registro. La autoridad de certificación puede firmar mensajes utilizando la clave pública pk^{CA};

- unas tarjetas de prepago disponibles en las gasolineras, quioscos o similares. Cada tarjeta incluye un código único y la CA asocia a cada código Pay.Code una cuenta con el crédito disponible;

- algún sistema para penalizar o prevenir el abuso del carril de transporte colectivo por parte de los vehículos, por ejemplo;

- una penalización sobre el importe en la fase de pago; y

- un mecanismo en el carril de transporte colectivo que impida el acceso a vehículos que han cometido algún tipo de abuso.

Tecnologías de comunicación utilizadas:

Los dispositivos móviles y en general los dispositivos de computación autónomos que pueden utilizar los ocupantes del vehículo deben disponer de algún medio de comunicación que les permita comunicarse entre ellos y con el puesto de peaje, ya sea utilizando tecnologías de comunicación en sí conocidas como RFID, Bluetooth, Wi-Fi u otras. La comunicación entre los dispositivos móviles debe incluir algún mecanismo que limite físicamente o lógicamente la distancia máxima de comunicación. Bluetooth

puede ser una solución tecnológica natural para el correcto funcionamiento del sistema, pero no se descartan otras.

Técnicas criptográficas preliminares

En criptografía de clave pública basada en identidad, las claves públicas corresponden a cadenas arbitrarias de longitud especificada, que se conocen como 'identidades'. Normalmente cada cadena de clave pública se asocia a un ocupante y refleja algún aspecto de la identidad del ocupante que lo identifica únicamente, por ejemplo, la dirección de correo electrónico. La clave secreta asociada a la clave pública de un ocupante *U* es calculada por alguna entidad de confianza, la autoridad de certificación *CA*, y es enviada a *U* por algún medio seguro. Una característica de la criptografía de clave pública basada en identidad muy interesante para la presente invención es que las claves públicas pueden ser muy cortas. La idea de la criptografía basada en identidad se debe a Shamir [3], quien en 1984 propuso la idea de simplificar la gestión de los certificados en las tradicionales infraestructuras de clave pública.

En los protocolos de criptografía de clave pública de umbral algunas tareas se distribuyen entre un grupo *n* de ocupantes de modo que al menos *t*, el umbral, ocupantes tienen que cooperar para hacer la tarea satisfactoriamente. Normalmente, en estos protocolos *n* y *t* se deciden al inicio del protocolo y no pueden ser modificados a menos que se vuelva a calcular toda la información pública de los ocupantes. La literatura relativa a protocolos criptográficos distribuidos es muy amplia.

Las firmas de clave pública de umbral dinámico (firmas identity-based dynamic threshold o IBDT) son como firmas digitales estándar exceptuando que: a) están basadas en la identidad, es decir, las claves públicas son cadenas arbitrarias de longitud especificada; b) son firmas de umbral, es decir, al menos *t* firmantes fuera del conjunto *S* de *n* firmantes tienen que colaborar para producir una firma válida; y c) el umbral es dinámico, lo que significa que el conjunto de firmantes *S* y el umbral *t* se pueden elegir en el momento del cálculo de la firma, es decir, pueden ser diferentes para cada firma. Un concepto similar se consideró en [1], pero para el cifrado en lugar de la firma y para el escenario de clave pública en lugar de un escenario basado en la identidad.

Informalmente, las propiedades de seguridad de un esquema de firma IBDT garantizan que al menos *t* ocupantes de un conjunto *S* han utilizado el algoritmo de firma con sus respectivas claves secretas para calcular la firma. Si el conjunto *S* de *n* firmantes son los ocupantes de un vehículo y calculan una firma con umbral *t=n*, la firma puede considerarse como una prueba de que como mínimo hay *n* ocupantes en el coche.

Una firma con umbral dinámico basada en identidad consiste en cinco algoritmos:

IBDTS=(IBDT.Setup,IBDT.Keygen,IBDT.Sign,IBDT.Comb,IBDT.Verify). El primer algoritmo simplemente devuelve los parámetros del esquema. *IBDT.Keygen* es el algoritmo que utiliza la autoridad de certificación para distribuir las claves secretas de los ocupantes. *IBDT.Sign* es un algoritmo que es ejecutado individualmente por los ocupantes y que devuelve una firma parcial. Al menos *t* ocupantes del conjunto de firmantes *S* deben ejecutarlo. El algoritmo *IBDT.Comb* toma *t* de estas firmas parciales y devuelve la firma final para el conjunto *S* y el umbral *t*. *IBDT.Verify* es un algoritmo que verifica si una firma dada es válida para un cierto conjunto *S* y umbral *t*.

Seguidamente se detallan los diversos protocolos empleados en la implementación del método expuesto.

Protocolos para el cobro en un peaje de vehículos de alta ocupación: caso sin tiquete de entrada

El primer protocolo es ejecutado por la autoridad de certificación y un ocupante que quiere utilizar el sistema de pago automático. Sólo es preciso ejecutarlo una vez por cada ocupante *U*.

Protocolo 1, o protocolo de registro. Al inicio del protocolo *CA* escoge un valor ℓ que debe ser menor que la longitud del número del documento nacional de identidad n_U. Véase Nota 9.1 sobre el valor apropiado de ℓ.

1. Un ocupante *U* con número de documento nacional de identidad n_U se autentica en una autoridad certificadora *CA*, en persona o por algún otro medio aceptable. El ocupante recibe un número de identificación personal pin_U.

2. La *CA* asocia a *U* un vector de claves públicas de Π,

$$\mathbf{PK} = (pk_1^{d_1}, \ldots, pk_\ell^{d_\ell}),$$

donde $d_1,\ldots,d_\ell$ son los últimos ℓ dígitos de n_U y Π es un esquema de firma digital IBDT. La clave pública $pk_i^{d_j}$ es una cadena corta que codifica *i* y d_j, por ejemplo concatenándolos:

$$pk_i^{d_j} = \frac{i}{d_j}.$$

3. Utilizando la clave privada maestra del esquema de firma digital Π, la *CA* calcula las claves secretas asociadas a ***PK***, las cuales son:

$$\mathbf{SK} = (sk_1^{d_1}, \ldots, sk_\ell^{d_\ell}).$$

4. Utilizando el número de identificación personal pin_U, el ocupante puede descargar en su dispositivo móvil la aplicación con las claves asociadas *SK* y la clave pública pk^{CA} de la autoridad certificadora.

El segundo protocolo simplemente especifica el modo en que un ocupante puede comprar de forma anónima crédito para pagar peajes.

Protocolo 2 Compra de crédito

El ocupante compra una tarjeta prepago para el sistema de pago de peajes, por ejemplo, una tarjeta "rasca-rasca" (en la que un código está oculto por una capa retirable por rascado).

•La tarjeta incluye un código *Pay.Code* que deberá introducirse en la aplicación del dispositivo móvil.

El siguiente protocolo es ejecutado por los ocupantes de un vehículo antes de entrar en el carril de pago del peaje.

Protocolo 3 Configuración.

1. Un ocupante U^* entre los ocupantes $U_1,...,U_n$ que viajan juntos en el vehículo toma el papel principal. Este ocupante será el responsable de la mayor parte de la comunicación con el puesto de peaje. U^* configura su aplicación para ejecutarse en modo maestro y los otros ocupantes configuran sus aplicaciones para ejecutarse en modo esclavo.

2. Los ocupantes se ponen de acuerdo en un índice $j \in \{1,2,...,\ell\}$ tal que el j-ésimo dígito menos significativo del número de documento nacional de identidad sea diferente para cada ocupante. El j-ésimo dígito menos significativo del número del documento nacional de identidad n_{U_i} del ocupante U_i será llamado en adelante d_j^i.

El siguiente protocolo se ejecuta cuando el vehículo entra en un carril de peaje y realiza el pago del peaje.

Protocolo 4 Pago A: sin tiquete.

1. El puesto de peaje automático B detecta los identificadores Bluetooth de los ocupantes de un vehículo y les envía una marca de tiempo Time.Stmp.

2. Cada ocupante U_i ejecuta el algoritmo *IBDT.Sign* para calcular una firma de Π usando su clave secreta $sk_j^{d_j^i}$, en el mensaje

$$\text{Msg} = \langle \text{Time.Stmp} \,//\, \text{pk}_j^{d_j^1} \,//\, \ldots \,//\, \text{pk}_n^{d_j^n} \rangle,$$

para el grupo de claves públicas $\{pk_j^{d_j^1}, \ldots, pk_n^{d_j^n}\}$ y el umbral *n* y donde // es una operación de concatenación. Seguidamente, envía la firma parcial resultante (σ_i) a U^*.

3. U^* recibe $(\sigma_1, \ldots, \sigma_n)$ y ejecuta el protocolo *IBDT.Comb* para combinar las firmas

parciales y obtener la firma final resultante (en nombre de $U_1,...,U_n$. Posteriormente, envía mensaje y firma al puesto de peaje B:

$$" < \mathbf{Msg}", (" > ".$$

4. El puesto de peaje verifica la firma mediante la ejecución de

$$\left[\text{IBDT. Verify}(\text{Msg}, \frac{(, \text{pk}]_j^{d_j^1}}{\square}, n \right.$$

$$\left. \frac{\cdots}{\text{pk}_j^{d_j^n}} \right)$$

Nótese que esta firma solamente será válida si todos los U1,...,Un han colaborado en su elaboración, con lo que se demuestra que en el vehículo hay por lo menos n ocupantes. Si la firma no es válida, el vehículo será penalizado de alguno de los modos propuestos anteriormente. En caso contrario, se calcula el importe total amount_n que un vehículo debe pagar en función del número de ocupantes del mismo, es decir, a mayor n, menor será el importe.

5. Cada ocupante *U* del vehículo que está en el conjunto *P* de ocupantes que quieren colaborar en el pago del peaje envía al puesto de peaje vía Bluetooth su código de pago cifrado con la clave pública del peaje:

$$\text{"C"}_{\downarrow}\text{"U"} \; " = " \; [\![\text{"Enc"}]\!]_{\downarrow}([\![\text{"pk"}]\!]^{\uparrow} CA \,) \text{"(Time. Stmp"// } [\![\text{"Pay. Code"}]\!]_{\downarrow} U),$$

donde Pay.Code_U es el código que el ocupante U obtiene de la tarjeta de prepago y donde Enc es el algoritmo de cifrado de clave pública de algún esquema de cifrado de clave pública Π'.

6. El puesto de peaje descifra los datos recibidos $\{c_U : U(P)\}$, para obtener los códigos de pago de los ocupantes en P.

7. El puesto de peaje resta la cantidad "amount_n" dividida por el cardinal de P de las cuentas asociadas a los códigos de pago recibidos.

Protocolos para el cobro en un peaje de vehículos de alta ocupación: caso con tiquete de entrada

Los Protocolos 1 y 2 son idénticos al caso sin tiquete y la única diferencia está en la fase de pago. En caso de cobrarse el peaje usando algún sistema de tiquetes, la fase de pago se divide en dos protocolos: el primero se ejecuta cuando los vehículos entran en el carril para vehículos de alta ocupación (VAO) y el segundo a su salida.

Protocolo 5 Pago B: entrada.

1. Un peaje automático B_1 situado a la entrada del carril detecta los identificadores Bluetooth de los ocupantes de un vehículo y les envía una marca de tiempo y un identificador de ubicación *Loc*

$$\mathrm{Msg}_{entry} = <\mathrm{Time.\,Stmp}_{entry}, \mathrm{Loc}>.$$

2. Cada ocupante U que está en el subconjunto P de ocupantes del vehículo que quieren colaborar en el pago del peaje envía al ocupante que actúa con el rol de maestro U^* el mensaje

$$\mathbf{C}_{U,entry} = \mathrm{Enc}_{\mathrm{pk}^{CA}}(\mathrm{Msg}_{entry}//\mathrm{Pay.\,Code}_U),$$

donde $\mathrm{Pay.\,Code_U}$ es el código que el ocupante U obtiene de la tarjeta prepago y Enc es el algoritmo de cifrado de algún esquema de clave pública Π'.

3. U^* envía al puesto de peaje:

$$\mathbf{C_{entry}} = <\mathbf{C_{U_{i_1}}}//\ldots//\mathbf{C_{U_{i_p}}}//\frac{\frac{\mathrm{pk}_j^{d_j^1}}{\square}}{\ldots}\Big/\frac{}{\mathbf{pk}_j^{d_j^n}}>$$

donde $P = \{U_{i_1}, \ldots, U_{i_p}\}$ es el conjunto de todos los ocupantes que quieren colaborar en el pago del peaje.

4. El puesto de peaje B_1 devuelve un tiquete $\mathrm{ticket} = \mathrm{Sign}_{sk^{CA}}(\mathbf{C}_{entry})$, donde Sign es algún algoritmo de firma de clave pública de algún esquema de firma digital ∑.

5. U^* almacena el tiquete ticket y $\mathbf{C}_{entry}$.

Protocolo 6 Pago B: salida.

1. Un peaje automático B_2 detecta los identificadores Bluetooth de los ocupantes de un vehículo y les envía una marca de tiempo *Time.Stmp*.

2. Cada ocupante U_j ejecuta el algoritmo IBDT.Sign para calcular una firma de Π utilizando su clave secreta $\mathbf{sk}_j^{d_j^i}$, en el mensaje

$$\mathbf{Msg} = <\mathrm{Time.\,Stmp}//\frac{\frac{\mathrm{pk}_j^{d_j^1}}{\square}}{\ldots\frac{\square}{\mathrm{pk}_n^{d_j^n}}}>,$$

para el grupo de claves públicas $\{pk_1^{d_j^1}, \ldots, pk_n^{d_j^n}\}$ y umbral n. Seguidamente, envía la firma parcial resultante $(\iota i$ a U^*.

3. U^* recibe "(" $(\iota "1", \ldots, (\iota "1"\ ")"$ y ejecuta el protocolo IBDT.Comb para combinar dichas firmas y obtener la firma final (en nombre de U1,...,Un. Entonces U^* envía al puesto de peaje B_2 el mensaje

" < Msg, "(, "C" $_\iota$*entry*, "ticket >."

4. Cada ocupante U del vehículo que está en el conjunto P de ocupantes que quieren colaborar en el pago del peaje envía al puesto de peaje vía Bluetooth su código de pago cifrado con la clave pública del peaje.

$$c_U = \mathrm{Enc}_{pk_{CA}}(\mathrm{Time.\ Stmp}//\mathrm{Pay.\ Code}_U),$$

donde Enc es el algoritmo de cifrado de clave pública de un esquema de cifrado de clave pública.

5. El peaje B_2 penaliza al vehículo en cualquiera de los siguientes casos:

- La firma (de *Msg* o la firma de *ticket* de C_{entry} no son válidas.

- Los códigos de pago cifrados dentro de C_{entry} difieren de los cifrados en $\{c_U : U \in P\}$.

- Las claves públicas especificadas en *Msg* difieren de las claves públicas en C_{entry}

6. En caso contrario, el peaje supone que hay n ocupantes en el vehículo y procede como en el Protocolo 4 para restar el importe amount_n dividido por el cardinal de P de cada cuenta asociada con cada código de pago recibido.

A continuación se detallan varias cuestiones de detalle de los protocolos especificados anteriormente.

Alcance de difusión

Tal como se ha mencionado en el apartado de descripción del sistema, para la seguridad del protocolo es importante que en la comunicación entre el puesto de peaje y los dispositivos móviles existan limitaciones de alcance, así como en la comunicación entre los propios dispositivos móviles en la fase de firma del protocolo de pago. El alcance de la difusión de los mensajes entre los dispositivos móviles puede ser limitado mediante tecnología, como por ejemplo si la comunicación se realiza con tecnología RFID. En este caso, ningún dispositivo vecino recibiría los mensajes.

Variantes del esquema de pre-distribución de claves

El número del documento nacional de identidad n_U puede ser reemplazado por cualquier número o cadena que identifique al ocupante de manera única.

El protocolo falla si no hay $j \in \{1,\ldots,\bullet\}$ tal que el j-ésimo dígito menos significativo de n_U sea distinto para todos los ocupantes del vehículo (la probabilidad de que esto pase se calcula en la Subsección 9.2). Para minimizar dicha probabilidad se podría asociar una clave a más de un dígito de n_U, por ejemplo.

Comunicación en caso de usar tecnología Bluetooth

El peaje debería detectar y comunicarse con los dispositivos móviles de un vehículo vía Bluetooth cuando accedan al carril de peaje, para que puedan recibir la marca de tiempo y hacer las operaciones necesarias de cifrado. En general, la fase de descubrimiento y comunicación entre dos dispositivos puede llegar a 20 segundos, lo cual no es lo suficientemente rápido para los propósitos de esta invención. Para acelerarlo, basta con que el peaje que tiene que descubrir los otros dispositivos Bluetooth (los dispositivos de los ocupantes de un vehículo) aumente la frecuencia de solicitud de identificación. De acuerdo con [2], en este caso el proceso puede llegar a tardar sólo 1,075 segundos y puede acelerarse hasta tardar un tiempo de 0,005 segundos siguiendo las optimizaciones propuestas en dicho artículo. Nótese que esta solución no es problemática en el presente caso ya que el puesto de peaje puede ser un dispositivo con alta capacidad de cálculo y sin restricciones de energía.

Claves públicas del peaje

También podría considerarse una variante del protocolo en la que cada puesto de peaje tuviera una clave pública diferente. Por ejemplo, esto podría ser necesario si los puestos de peaje perteneciesen a varias empresas de cobro. En este caso, cuando el coche entra en el carril el puesto de peaje envía a sus ocupantes su clave pública junto con un certificado válido. Ambos protocolos (con tiquete o sin tiquete) continúan como se ha detallado más arriba, excepto que ahora los códigos de pago están cifrados con la clave pública que el puesto de peaje ha emitido en lugar de pk^{CA}.

A continuación se detallan algunos aspectos técnicos de los protocolos.

Corrección

La corrección garantiza que cualesquiera n ocupantes $U_1,\ldots,U_n$ que sigan correctamente el protocolo podrán convencer al puesto de peaje de que hay por lo menos n ocupantes en el vehículo. El único paso en el que la prueba puede fallar es cuando por cada uno de los últimos ℓ dígitos de los números del documento nacional de identidad exista algún valor repetido entre los ocupantes del vehículo. En este caso, para cada $j \in \{1,\ldots,\bullet\}$, el conjunto de claves $\{pk_j^{d_j^1},\ldots,pk_j^{d_j^n}\}$ tiene a lo sumo n' elementos diferentes para algunos $n'<n$ y sólo será posible generar una firma que pruebe que en el coche hay al menos n' ocupantes. La probabilidad de que esto pase depende de ℓ (el número de claves que se le da a cada ocupante) y n (el número de ocupantes que se encuentran en el vehículo); más concretamente, suponiendo $n \leq 10$, dicha probabilidad es:

$$F(\ell,n)=\left(1-\frac{10(10-1)\ldots(10-n+1)}{10^n}\right)^{\ell}.$$

Si el número de ocupantes n es cercano a 10, la probabilidad de fallo anterior puede ser no despreciable para valores razonables de ℓ. Una opción que permite incrementar n incluso muy por encima de 10 es asociar cada clave pública no a un solo dígito del documento nacional de identidad, sino a m dígitos. En este caso, suponiendo $n \leq 10^m$ la probabilidad de fallo es:

$$F(\ell,n,m)=\left(1-\frac{10^m(10^m-1)\ldots(10^m-n+1)}{10^{nm}}\right)^{\ell}.$$

Sin embargo, el precio a pagar por la elección de un valor m mayor es la reducción del anonimato, ya que si más dígitos están asociados a cada clave pública, menos ocupantes comparten la misma clave pública. Si se desea admitir un máximo de 9 ocupantes, tomar m=2 debería ser suficiente.

Aspectos de seguridad

La fase de registro asegura que cada ocupante U se asocia a un sólo dispositivo móvil. Por otro lado, las limitaciones en el alcance de las comunicaciones entre los dispositivos garantizan que solamente los dispositivos que están en el vehículo han colaborado para calcular la firma final de (. Nótese que sin la limitación en el alcance de las comunicaciones, algún ocupante de un vehículo cercano podría participar con su dispositivo en el protocolo de firma. Finalmente, las propiedades de seguridad del esquema de firma garantizan que cualquier firma de los firmantes con la claves públicas $\mathbf{pk}_1^{d_i^1}, \ldots, \mathbf{pk}_n^{d_i^n}$ y umbral n sólo se verificará correctamente si por lo menos n ocupantes diferentes han colaborado en calcularla. Por lo tanto, debe haber por lo menos n dispositivos electrónicos registrados en el vehículo, lo que significa que también hay por lo menos n *ocupantes diferentes* a menos que algún ocupante registrado que no esté en el vehículo haya prestado su dispositivo móvil a los otros ocupantes. El esquema propuesto aquí no detecta este tipo de mal comportamiento, pero no esperamos que este ataque sea común, ya que la mayoría de las personas se resisten a prestar sus dispositivos móviles.

En un peaje con tiquete, un posible ataque sería que dos vehículos intercambiaran sus tiquetes de entrada con el objetivo de pagar menos si presentan el tiquete equivocado. Este ataque sólo tendrá éxito si en el peaje de salida no se detecta el fraude, lo que implicaría que los ocupantes de ambos vehículos tuvieran el mismo conjunto de claves públicas y también que intercambiaran sus códigos de pago Pay.Code (ya que tienen que enviarlos cifrados con la marca de tiempo obtenida en la salida). No parece esperable que los ocupantes quieran compartir sus códigos de pago.

Anonimato

El protocolo expuesto garantiza el anonimato de los ocupantes en el sentido de que no es posible para un intruso o incluso para el propio puesto peaje identificar a los ocupantes del vehículo dentro de un grupo muy grande de ocupantes. De hecho, debe tenerse en cuenta que la única información que ve el puesto de peaje acerca de los ocupantes es su código de pago, su identificador de red (por ejemplo

identificador Bluetooth) y el conjunto de claves públicas $\left[PK = \{pk]_i^{d_1}, \ldots, pk_i^{d_n}\right\}$ asociadas a la firma. Ahora bien:

Los códigos de pago pueden comprarse anónimamente (abonando la tarjeta de prepago en efectivo) y por lo tanto los códigos de pago no están directamente vinculados a ningún ocupante.

Los identificadores de red pueden ser escogidos por los ocupantes de forma arbitraria y pueden elegirse de modo que no exista una relación obvia con la identidad del propietario del dispositivo.

Por otro lado, cualquiera de las claves en el conjunto $\mathcal{PK}$ es compartida con todos los ocupantes que tienen el mismo dígito en la posición i de su número de documento nacional de identidad. Por ejemplo, en el caso de España, donde el número del documento nacional de identidad tiene ocho dígitos, para cualquier par i,d puede haber hasta 10^7 ciudadanos (10^6 si asociamos las claves con dos dígitos) compartiendo la clave pública $\mathbf{pk}_i^d$. En la práctica no habrá tantos ciudadanos compartiendo una clave pública porque no todos los números corresponden a un documento nacional de identidad emitido y no todo el mundo con un documento registrará su dispositivo móvil; aun así el número de ocupantes con la misma clave pública seguirá siendo alto.

Referencias

[1] C. Delerablée and D. Pointcheval. Dynamic threshold public-key encryption. In Advances in Cryptology - CRYPTO 2008, LNCS 5157, pp. 317–334, Springer, 2008.

[2] J-R. Jiang, B-R. Lin, and Y-C. Tseng. A mechanism for quick Bluetooth device discovery. In Proceedings of Mobile Computing 2004, Taichung, Taiwan, March 2004.

[3] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology - CRYPTO 1984, LNCS 196, pp. 47–53, Springer, 1984.

REIVINDICACIONES

1.- Método de cobro sin contacto, por el uso de una vía, para vehículos de alta ocupación, en donde cada uno de los ocupantes de un vehículo que implementa el método de cobro posee un dispositivo de computación autónomo con capacidad de telecomunicación, identificable mediante un identificador individual Id o dirección de red, comprendiendo el método determinar el número de ocupantes de un vehículo utilizando información acerca de dichos dispositivos de computación autónomos con capacidad de telecomunicación, mediante una interacción sin contacto con los mismos desde un centro de control de la vía o estación de cobro, para proporcionar un importe del pago por el uso de la vía, en función del número de ocupantes del vehículo, caracterizado porque dicha determinación del número de ocupantes se lleva a cabo por la adquisición y recuento de un número total de firmas digitales parciales realizadas por cada ocupante mediante una aplicación informática albergada en su respectivo dispositivo de computación autónomo con capacidad de telecomunicación, en donde dicha aplicación informática implementa un esquema de firma digital basado en la identidad, con umbral dinámico, que garantiza el anonimato de dichos ocupantes del vehículo y la seguridad de la interacción centro de control-ocupantes.

2.- Método, según la reivindicación 1, caracterizado porque cada ocupante del vehículo adquiere una cantidad a modo de crédito que le proporciona un código de pago y el pago se realiza en dicho centro de control, sin contacto, por parte de uno o más de los ocupantes, desde su dispositivo de computación autónomo con capacidad de telecomunicación, conservando el anonimato.

3.- Método, según la reivindicación 1, caracterizado porque dicha interacción sin contacto centro de control-ocupantes comprende la participación de una autoridad certificadora que proporciona a cada uno de los ocupantes del vehículo un conjunto de claves públicas y claves privadas para realizar las citadas firmas digitales parciales.

4.- Método, según la reivindicación 1, en donde dicha vía de pago es una vía de peaje de tarificación variable en función del número de ocupantes de cada vehículo que cruza el peaje, y en el cual intervienen al menos los siguientes agentes:

una estación para cobro de un peaje con medios de telecomunicación;

un dispositivo de computación autónomo, para cada uno de los ocupantes, con capacidad de telecomunicación, con un identificador individual Id o dirección de red;

una autoridad certificadora que proporciona un conjunto de claves públicas y claves privadas para realizar dichas firmas digitales parciales; y

al menos una aplicación informática instalable en los dispositivos de computación autónomos para implementar el método mediante dichos dispositivos de computación autónomos,

caracterizado por comprender las siguientes etapas:

a) autenticación ante una autoridad certificadora de cada uno de los n ocupantes del vehículo a partir de dicho identificador individual que asocia a la identidad del ocupante del vehículo un único número Id, de misma longitud;

b) generación para cada ocupante de un conjunto de L claves públicas y las correspondientes claves privadas por parte de dicha autoridad certificadora, en donde para i=1 hasta L el par i-ésimo de claves es solamente función del valor del i-ésimo dígito (o del i-ésimo grupo de dígitos) menos significativo de Id;

c) transferencia de dichas claves privadas generadas a su respectivo ocupante;

d) adquisición por cada ocupante de una cantidad a modo de crédito que proporciona un código de pago;

e) uno de los ocupantes del vehículo Um (maestro) adopta un papel principal y cada uno de los ocupantes del vehículo establece un dígito/posición o grupo de dígitos/posiciones de cada uno de sus identificadores personales Id, que sea distinto para cada uno de dichos ocupantes, sea esta posición/grupo la j-ésima;

f) la estación de peaje proporciona para cada vehículo próximo a la estación de peaje un identificador de transacción Ts con una marca de tiempo;

g) cada uno de los ocupantes del vehículo realiza una firma parcial con umbral n (siendo n el número de ocupantes del vehículo) con su clave privada j-ésima del mensaje formado por Ts concatenado con las claves públicas j-ésimas de todos los ocupantes y se envían dichas firmas parciales;

h) adquisición o recepción por dicha estación de peaje de una firma final en nombre del grupo, a partir de las citadas firmas parciales;

i) verificación por parte de dicha estación de peaje de dicha firma final de grupo, cual firma solo será válida si han participado en ella n ocupantes, con lo que permite determinar de forma segura y anónima el número n de ocupantes del vehículo, y

j) aplicación por parte de la estación de peaje de un importe prestablecido conforme a unos baremos tarifarios según el número de ocupantes, y petición de dicha cantidad a los ocupantes del vehículo para habilitar un pago.

5.- Método según la reivindicación 4, caracterizado porque dicho envío de las firmas parciales de la etapa g) se realiza por parte de cada uno de los ocupantes a un ocupante Um, el cual combina las firmas parciales y obtiene una firma final de grupo, representativa de los n ocupantes, que es enviada a la estación de peaje.

6.- Método según la reivindicación 4, caracterizado porque dicho envío de las firmas parciales de la etapa g) se realiza por parte de cada ocupante del vehículo a la estación de cobro de un peaje, en donde se combinan las firmas parciales y se obtiene una firma final de grupo, representativa de los ocupantes.

7.- Método según la reivindicación 4, caracterizado porque el pago es asumido por uno o más ocupantes del vehículo que se dividen el importe a pagar que es transferido de forma segura a partir de uno de los dispositivos de computación autónomos, en particular del de dicho Um.

8.- Método según la reivindicación 4, caracterizado porque dicha adquisición de una cantidad a modo de crédito de la etapa d) es realizada de manera anónima.

9.- Método según la reivindicación 4, caracterizado porque dicha adquisición de una cantidad a modo de crédito de la etapa d) es realizada a través de una tarjeta de crédito.

10.- Método según la reivindicación 4, caracterizado porque la citada transferencia de dichas claves privadas de la etapa c) se realiza por parte de una oficina bajo un esquema presencial o por conexión remota con la misma e identificación segura por parte de un ocupante o potencial ocupante del vehículo.

11.- Método según la reivindicación 4, caracterizado porque dicha etapa f) se realiza contemporáneamente ante una petición de pago o detección de un vehículo por parte de la estación de peaje.

12.- Método según la reivindicación 4, caracterizado porque dicha etapa e) se realiza en cualquier momento de formación o consolidación de la agrupación de ocupantes del vehículo, en un momento dado.

13.- Método según la reivindicación 4, caracterizado porque para implementar dicha etapa f) la estación de peaje detecta los identificadores Id de dichos dispositivos de computación autónomos con capacidad de telecomunicación de los ocupantes del vehículo, reconoce el número de dispositivos que viajan en el vehículo y les envía un identificador de transacción Ts con marca de tiempo.

14.- Método según la reivindicación 4, caracterizado porque la estación de peaje realiza previamente a dicha etapa f) un envío de solicitud de pago al ocupante Um.

15.- Método según la reivindicación 5, caracterizado porque en el caso de pago utilizando tiquetes, una marca de tiempo Msg y un localizador de referencia de un peaje de entrada, son enviados por una estación de peaje de entrada a los ocupantes del vehículo y cada ocupante de los que va a colaborar en el pago envía dicha Msg concatenada con un código de pago y cifrado con la clave pública del peaje al ocupante Um.

16.- Método según la reivindicación 15, caracterizado porque el ocupante Um o la estación de peaje concatena todos los mensajes cifrados recibidos de los ocupantes del vehículo que van a pagar junto con las claves públicas j-ésimas de los ocupantes, sea "Centry" el mensaje resultante de dicha concatenación, y la estación de peaje devuelve como tiquete el mensaje "Centry" recibido de los ocupantes firmado con la clave privada del peaje y el ocupante Um almacena Centry y el tiquete en su dispositivo de computación autónomo.

17.- Método según la reivindicación 16, caracterizado porque en la salida del peaje, en la etapa g) dicho ocupante Um envía además "Centry" y el tiquete.

18.- Método según la reivindicación 17, caracterizado porque en el momento de realizar el pago deben coincidir los ocupantes que se ofrecieron a pagar en la entrada con los que pagan en la salida, evitando cambios fraudulentos de tiquetes.

19.- Método según la reivindicación 4, caracterizado porque dicha etapa a) de autenticación de los n ocupantes del vehículo mediante su identificador Id, respectivo, solo es necesario realizarla una vez, por parte de cada uno de los ocupantes del vehículo.

20.- Método según una cualquiera de las reivindicaciones anteriores, caracterizado porque dicha interacción sin contacto utiliza una tecnología de telecomunicación conocida escogida entre Bluetooth, Wifi, RFID que soportan los dispositivos de computación autónomos con capacidad de telecomunicación de los ocupantes del vehículo.

21.- Sistema de cobro, sin contacto, por el uso de una vía, para vehículos de alta ocupación, que integra los siguientes elementos:

una estación para cobro de una tasa variable por el uso de la vía, con medios de telecomunicación;

un dispositivo de computación autónomo, para cada uno de los ocupantes, con capacidad de telecomunicación, con un identificador individual Id o dirección de red;

al menos una aplicación informática instalable en los dispositivos de computación autónomos con capacidad de telecomunicación, para implementar el método mediante dichos dispositivos de computación autónomos,

una autoridad certificadora que proporciona un conjunto de claves públicas y claves privadas para realizar dichas firmas digitales parciales; y

medios establecidos en un centro de control o centro de cobro para interacción bidireccional sin contacto de dicha estación para cobro por uso de la vía, con dichos dispositivos autónomos con capacidad de telecomunicación,

estando previstos dichos elementos, que operan en combinación, para implementar el método de cobro sin contacto según una cualquiera de las reivindicaciones 1 a 20.