(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 841**

(21) Número de solicitud: 201000865

(51) Int. Cl.:
H04W 12/00 (2009.01)
H04W 84/18 (2009.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **29.06.2010**

(43) Fecha de publicación de la solicitud: **27.01.2012**

(43) Fecha de publicación del folleto de la solicitud: **27.01.2012**

(71) Solicitante/s: **Universidad de La Laguna**
OTRI - Edificio Central
Delgado Barreto, s/n
38201 La Laguna, Tenerife, ES

(72) Inventor/es: **Caballero Gil, Pino;**
Caballero Gil, Cándido y
Molina Gil, Jezabel

(74) Agente: **No consta**

(54) Título: **Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada.**

(57) Resumen:
Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada, sin infraestructuras ni en carretera ni en vehículos, utilizando solamente dispositivos móviles con receptor de un sistema global de navegación por satélite, y capacidad de comunicación inalámbrica y de computación, tales como teléfonos móviles, PDAs y ordenadores portátiles. El modo de funcionamiento previsto en la invención es totalmente distribuido y descentralizado, y tiene en cuenta la protección de la privacidad de los conductores y la defensa ante posibles ataques.

ES 2 372 841 A1

DESCRIPCIÓN

Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada.

Sector de la técnica

Telecomunicaciones. Comunicaciones móviles e inalámbricas entre vehículos.

Introducción

La presente invención está relacionada con la seguridad de las comunicaciones en las redes *ad-hoc* vehiculares o VANETs (Vehicular *Ad-hoc* NETworks). Dicha seguridad representa actualmente un reto a resolver ya que se prevé que esas redes supondrán en un futuro no muy lejano una importante revolución para la seguridad y el confort del transporte por carretera.

En las VANETs los mensajes intercambiados entre los vehículos influirán en el comportamiento de sus conductores pues éstos por ejemplo, reducirán la velocidad y/o escogerán rutas alternativas en función de la información recibida. Cualquier usuario malintencionado podría intentar explotar esta situación, llevando a cabo alguno de los siguientes ataques:

- Inyección de información falsa, modificada o repetida, difundiendo datos erróneos que puedan afectar al resto de vehículos, bien en beneficio del atacante por ejemplo al conseguir liberar una vía, o simplemente por mala intención por ejemplo para producir un atasco.

- Falsificación de identidad (haciéndose pasar por ejemplo por un vehículo de emergencia) o manipulación de la información enviada (alterando datos como posición, dirección, velocidad, etc.) por ejemplo para intentar escapar de responsabilidades al haber provocado un accidente.

- Seguimiento de conductores y/o vehículos, amenazando su privacidad y anonimato.

- Denegación de servicio, provocando la pérdida de la conectividad de la red.

Por tanto, la seguridad de las comunicaciones es un factor imprescindible a la hora de impedir dichas amenazas y posibilitar el despliegue de las VANETs.

Aunque el planteamiento general de la invención puede ser usado en diferentes aplicaciones de las VANETs, los análisis llevados a cabo y la realización concreta descrita al final de este documento están centrados en la reducción de atascos en la carretera.

Estado de la técnica

Existen diversas iniciativas tanto desde la industria como desde el entorno académico destinadas a hacer posible la futura explotación de las VANETs. Sin embargo, todas las propuestas existentes tienen en común la hipotética existencia previa de una infraestructura en la carretera o RSU (Road-Side Unit) y/o el uso de telefonía móvil, y/o Internet y/o dispositivos a bordo de los vehículos u OBUs (On-Board Units).

Por ejemplo el borrador de estándar de comunicaciones para VANETs, IEEE 802.11p WAVE (Wireless Access for Vehicular Environments, http://grouper.ieee.org/groups/802/11/Reports) que está siendo desarrollado por el consorcio Car-2-Car (http://www.car-to-car.org) presupone que las VANETs combinarán varias tecnologías inalámbricas como Celular, Satélite, WiMAX (Worldwide Interoperability for Microwave ACCess, http://www.ieee802.org/16) y comunicaciones DSR (Dedicated Short Range).

De igual forma, la arquitectura CALM (Communications, Air interface, Long and Medium range, http://www.isotc204wg16.org/concept), también en proceso de estandarización por la organización ISO (International Organization for Standardization), pretende dar soporte a comunicaciones en entornos móviles y en particular en ITSs (Intelligent Transportation Systems), mediante el uso combinado de varias tecnologías inalámbricas como WAVE, UMTS (Universal Mobile Telecommunications System, http://www.3GPP.org), WiMAX o RFID (Radio Frequency IDentifícation), y la aplicación de diversos estándares internacionales, interfaces y medios, como IEEE 802.11, 802.11p, 802.15, 802.16e, 802.20, telefonía móvil 2G/3G/4G, e ITSs nacionales.

En ambos estándares, la seguridad de las comunicaciones se basa en la combinación de las tecnologías mencionadas, en general suponiendo el uso de infraestructuras de clave pública con certificación basada en autoridades centralizadas, lo que implica la necesidad de implementación previa de RSUs en carreteras y OBUs en vehículos.

Por otra parte, las soluciones propuestas en diversos proyectos de investigación se basan en la disponibilidad de OBUs en los vehículos, y/o de RSUs en la carretera, lo que implicaría un gran desembolso inicial por el Estado y/o por los usuarios. De hecho, la mayor parte de los esfuerzos investigadores en este campo se está haciendo desde las compañías automovilísticas, de forma que en las propuestas normalmente se supone que en las OBUs integradas en

los vehículos hay una caja negra, una identidad certificada, sensores para detectar obstáculos, una interface humano-máquina, y un dispositivo a prueba de falsificaciones para hacer los cálculos, además de un receptor de un Sistema Global de Navegación por Satélite y un dispositivo Wi-Fi.

Entre las publicaciones científicas relacionadas con la seguridad en las VANETs, destacan las siguientes:

- Philippe **Golle**, Dan **Greene** and Jessica **Staddon**, "Detecting and correcting malicious data in VANETs", *1st ACM international workshop on Vehicular ad hoc networks* pp. 29-37. 2004. Propone el uso de sensores para detectar información incorrecta.

- Maxim **Raya** and Jean-Pierre **Hubaux**, "The security of vehicular *ad hoc* networks", *3rd ACM workshop on Security of ad hoc and sensor networks* pp. 11-21. 2005. Asume la existencia de autoridades de certificación para emitir los certificados a los vehículos, proponiendo que sean las autoridades gubernamentales o los fabricantes de vehículos.

- Florian **Dötzer**, "Privacy Issues in Vehicular *Ad Hoc* Networks", *Lecture Notes in Computer Science* 3856 pp. 197-209. 2006. Supone la participación de los fabricantes de vehículos ya que durante la producción de cada vehículo se debe establecer una conexión segura con una autoridad certificadora que valide la OBU.

Entre las patentes destacan los siguientes documentos relacionados con las VANETs.

US2008002635 y US2008002574 proponen un método para gestionar el tráfico de comunicaciones, midiendo niveles locales y definiendo una microutilidad de los datos a transmitir para seleccionar el medio de transmisión.

US20080279141 describe un método de asignación de canales a las comunicaciones multihop entre un nodo y otro, para el envío de información mediante enrutamiento.

WO2008092475 propone la diseminación de información mediante unicast.

WO2008104673 plantea la estimación de la densidad de nodos mediante la división en celdas geográficas en las que el nodo más cercano al centro es el encargado de agregar y retransmitir la información.

WO2008119948 se basa en el uso de telefonía móvil para definir un algoritmo de enrutamiento de información entre dos nodos.

WO2009024945 describe un método para sincronizar dispositivos comunicados por radio mediante beacons periódicos que incluyen señales de reloj.

WO2009053657 propone que en las intersecciones de carreteras el broadcast de información se realice a través de un nodo elegido dentro de un grupo en función del tiempo estimado para alcanzar la intersección.

WO2010020260 presenta un método para el envío de información desde un nodo origen hasta un nodo destino mediante enrutamiento a través de nodos intermedios.

WO2010040372 presupone el uso de una infraestructura en la carretera para controlar la carga de comunicaciones del canal inalámbrico, definiendo prioridades sobre los mensajes para establecer sus características de envío.

Sin embargo, no se ha encontrado ningún precedente que describa una solución segura y más económica que las propuestas hasta ahora. En este sentido nuestra invención evita la necesidad de instalar ningún tipo de infraestructura ni en el vehículo ni en la carretera, lo que implica un ahorro en inversión económica y en tiempo de espera para el desarrollo de las múltiples aplicaciones de las redes vehiculares, permitiendo poner en marcha las VANETs sin ninguna inversión de gobiernos, compañías automovilísticas ni empresas de telefonía.

Se presenta aquí un sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada, sin infraestructuras ni en carretera ni en vehículos, utilizando solamente dispositivos móviles con receptor de un sistema global de navegación por satélite, y capacidad de comunicación inalámbrica y de computación, tales como teléfonos móviles, PDAs y ordenadores portátiles.

El modo de funcionamiento previsto en la invención es totalmente distribuido y descentralizado, y tiene en cuenta la protección de la privacidad de los conductores y la defensa ante posibles ataques. Ambas cuestiones implican la posibilidad de despliegue progresivo con funcionalidad efectiva y seguridad desde el primer momento.

Los factores clave del diseño propuesto son: escalabilidad y economía, autenticación de nodos e información, privacidad, fomento de la cooperación, y bajo retardo y estabilidad de las comunicaciones.

Se propone un sistema que puede integrarse en dispositivos móviles específicos, o bien implementarse en dispositivos ya existentes en el mercado como teléfonos móviles dotados de software adecuado.

Breve descripción de la invención

El primer elemento fundamental de la presente invención es un método de autenticación autogestionada, que no requiere de intervención de autoridades de certificación ya que son los propios nodos los que certifican la validez de las claves públicas de los nodos en quienes confían, emitiéndoles los correspondientes certificados, que son guardados en almacenes locales y actualizados mediante un algoritmo aquí descrito. Además, la propuesta de autenticación de nodos incluye un protocolo criptográfico, que permite que cada nodo convenza a otro nodo de la posesión de cierto secreto sin que la información transmitida permita descubrir nada sobre dicho secreto, impidiendo posibles ataques de suplantación.

Un segundo elemento fundamental de esta invención es un algoritmo de cifrado simétrico utilizado en diferentes fases. Para su diseño se contemplan todos aquellos parámetros conocidos que garantizan la seguridad de los filtrados no lineales en cifrados en flujo.

Por último la presente invención contempla también como tercer elemento fundamental un esquema de agregación de datos que incluye la generación de paquetes agregados a partir de grupos creados *ad-hoc* para ello, y la verificación de las firmas digitales de forma probabilística.

En la presente invención se asume que cada nodo de la red está caracterizado por los siguientes parámetros:

$$ID, (KU_{ID}, KR_{ID}), \{ID_i, KU_{IDi}, Cert(KU_{IDi})\}_{IDi \in Almacén}$$

incluyendo:

- un IDentificador único (denotado ID), obtenido mediante la aplicación de una función unidireccional sobre un valor único. Por ejemplo, si el dispositivo usado es un teléfono móvil se puede usar el número, mientras que en otros casos se puede usar una dirección de correo electrónico. La función unidireccional podría ser una función hash, como por ejemplo MD5.

- un par fijo de claves pública/privada (denotadas (KU, KR) y llamadas claves de identidad para usar en un criptosistema asimétrico, como por ejemplo RSA.

- un almacén conteniendo varios IDs, y correspondientes claves públicas KUs y certificados, que el nodo mantiene en todo momento actualizado, de la forma:

ID1	KU_{ID1}, $Cert(KU_{ID1})$
ID2	KU_{ID2}, $Cert(KU_{ID2})$
ID3	KU_{ID3}, $Cert(KU_{ID3})$
.	.
.	.
.	.
IDlím	$KU_{IDlím}$, $Cert(KU_{IDlím})$

Descripción detallada de la invención

Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada que comprende los siguientes módulos (ver Figura 1):

C1. *Generación de claves de identidad y de firma digital*

Constituye parte del primer elemento fundamental de la invención. Dicha generación es necesaria ya que la autenticación de nodos propuesta en esta invención se basa en criptografía de clave pública autogestionada sin requerir en ningún momento autoridades de certificación. En su lugar, cada nodo es responsable de generar sus propios pares de claves pública/privada, que son imprescindibles para los procesos de autenticación, y de firma digital de los mensajes que envíe una vez autenticado. Cada nodo cuenta con un par fijo de claves pública/privada (claves de identidad) cuya validez es certificada de forma autogestionada mediante los almacenes de claves públicas de los propios nodos.

C2. *Arquitectura cliente/servidor con posibilidad de conexión a múltiples usuarios a la vez*

Es necesaria para el primer elemento fundamental de la invención. Consiste en que cada nodo (cliente) realiza peticiones a otro nodo (servidor), que le responde (ver Figura 2). Esta idea es muy útil en sistemas multiusuarios distribuidos tales como la red vehicular objeto de esta invención porque así la capacidad de proceso se reparte entre los clientes y los servidores. En particular en esta invención este componente es necesario para la interconexión de los nodos ya que permite enviar y recibir mensajes de muchos clientes y hacia muchos servidores a la vez pues cada usuario es a la vez cliente y servidor.

C3. *Envío multicast y recepción inalámbrica de beacons con seudónimos variables*

Es parte del primer elemento fundamental de la invención. El envío/recepción de mensajes beacons conteniendo seudónimos variables de los nodos emisores es necesario para el proceso de descubrimiento de nodos activos, y evitar posibles seguimientos (ver Figura 2).

C4. *Autenticación mutua de nodos, con intercambio de claves públicas fijas, claves secretas temporales, y almacenes de claves públicas*

Es la base del primer elemento fundamental de la invención. El intercambio de mensajes entre pares de nodos tiene como objeto que cada uno demuestre al otro que conoce un secreto sin revelarle nada sobre él. El esquema propuesto se basa en un esquema interactivo de reto-respuesta, según se muestra en la Figura 3. En el paso de envío de beacons cada nodo se compromete frente a sus vecinos con lo que pretende demostrar, enviándoles un testigo (D1). Si un nodo A desea establecer contacto con otro nodo B, le envía un reto aleatorio (D2). Entonces B devuelve la respuesta (D3) correspondiente al reto y al testigo. Tras dichos pasos, ambos nodos comparten una clave que usan para cifrar y enviar al otro su clave pública de identidad. A continuación se intercambian sus claves secretas temporales cifradas con la clave pública del otro nodo. Finalmente cada uno usa su propia clave secreta para cifrar y enviar cifrado el almacén de claves. Este módulo permite garantizar a cada nodo la autenticidad del otro, así como intercambiar las claves secretas que se usan en el módulo C7, y actualizar los almacenes de claves públicas necesarios para la posterior comprobación de la validez de las claves públicas de identidad usadas para la firma de mensajes.

C5. *Actualización óptima de los almacenes de claves públicas*

Es una parte importante del primer elemento fundamental de la invención. Permite limitar el número de claves almacenadas a un valor denotado lím, de manera que dicho valor sea en general inferior al número de usuarios que forman la red vehicular, e igual al mínimo número que permita, aprovechando la propiedad de los seis grados de separación consistente en que cualquier nodo puede conectarse a cualquier otro a través de una cadena con no más de seis enlaces (ver Figura 4), almacenar sólo las claves necesarias para poder autenticar a cualquier otro nodo con una alta probabilidad.

C6. *Esquema de reputación de nodos, que borra de los almacenes a los nodos deshonestos*

Forma parte del primer elemento fundamental de la invención. Permite aislar a aquellos nodos para los que se hayan detectado comportamientos incorrectos o corruptos, mediante el borrado de su clave pública de los almacenes de certificados.

C7. *Intercambio cifrado de datos sobre elementos estáticos y dinámicos de la carretera*

Este módulo constituye el segundo elemento fundamental de la invención. El intercambio cifrado de la información obtenida sobre la carretera y el tráfico, que tengan almacenada en ese momento los nodos es necesario para evitar comportamientos pasivos de usuarios que pretendan aprovecharse de la VANET sin cooperar para su funcionamiento. El uso de un criptosistema de clave secreta es recomendable dada la dimensión del fichero de datos. Nuestra invención propone para ello usar una clave secreta temporal del emisor.

C8. *Autenticación de datos*

El tercer elemento fundamental de la invención es parte de este módulo. Para el buen funcionamiento de la red es imprescindible la verificación de integridad y origen de los datos recibidos mediante firma digital, evaluación de características verificables (frescura, localización, relevancia, corrección, etc.) y comprobación de coincidencias con agregación, ya que se debe comprobar en todo momento que la información retransmitida es auténtica, actual y válida. En esta invención autogestionada esto es sólo posible combinando técnicas de verificación de integridad y origen, evaluación de características verificables, y comprobación de coincidencias con otros mensajes recibidos mediante agregación de datos.

Descripción de las figuras

Figura 1: Esquema conceptual del sistema incluyendo sus 8 módulos básicos de Generación de claves y firma (C1), Arquitectura cliente/servidor (C2), Envío y recepción de beacons (C3), Autenticación de nodos (C4), Actualización de almacenes (C5), Esquema de reputación (C6), Intercambio cifrado (C7) y Autenticación de datos (C8). La ejecución de

dichos módulos no es necesariamente secuencial, ya que C5 y C6 no requieren interacción entre nodos, mientras que C7 y C8 sí, de forma que C5 y C6 pueden ejecutarse en paralelo con C7 y C8. De hecho, en la propuesta de realización descrita se proponen dos modos tales que en uno de ellos no se requiere la ejecución de los módulos C7 y C8.

Figura 2: Esquema que representa la arquitectura cliente/servidor con conexión a múltiples usuarios a la vez, y también el envío multicast y recepción inalámbrica de los beacons.

Figura 3: Esquema de autenticación mutua basada en una demostración interactiva de conocimiento nulo entre un par de nodos A y B. En el paso de envío de beacons B se compromete frente al nodo A con el objeto a demostrar enviándole un testigo (D1). Si A desea establecer contacto con B, le envía un reto aleatorio (D2). Finalmente B devuelve la respuesta (D3) correspondiente al reto y al testigo.

Figura 4: Esquema que representa la propiedad de los seis grados de separación en el entorno de la certificación de claves públicas entre vehículos.

Figura 5: Esquema que muestra la propuesta de realización de la invención utilizando el teléfono móvil asociado en primer lugar al dispositivo manos libres de un vehículo, de forma que antes de poner en marcha el vehículo el usuario introduce su destino y preferencia de ruta, y cuando el móvil recibe información sobre velocidades anormales de sus vecinos, recalcula la ruta recomendada y se la sugiere al conductor.

Figura 6: Ejemplificación de la generación propuesta de la clave pública de identidad KU_{ID} a partir de un grafo y su matriz de adyacencia, usando los elementos de la submatriz triangular superior correspondientes a un circuito hamiltoniano en el grafo.

Figura 7: Esquema que representa todas las interacciones entre dos nodos A y B. Primero A envía a B el hash $\{\forall ID \in Almacén_A\}$ (P1), en el paso (P2) B solicita al nodo A el listado de IDs de su almacén, luego A envía a B el conjunto $\{\forall ID \in Almacén_A\}$ (P3), B comprueba si hay una clave $X \in \{Almacén_A \cap Almacén_B\}$ y en ese caso se la envía al nodo A, (P4). Entonces A construye y envía a B un grafo $G_A(X)$ (P5). Después se realizan al menos dos iteraciones de tres pasos en los que primero A envía a B un grafo $GI_A(X)$ (P6) isomorfo al grafo $G_A(X)$, luego B envía al nodo A un reto binario aleatorio (P7), y según su valor A devuelve a B el isomorfismo entre ambos grafos o un circuito hamiltoniano en $GI_A(X)$ (P8). Al finalizar, A usa X para cifrar su clave KU_A y enviar a B el resultado $Ex(KU_A)$ (P9), luego B usa la clave KU_A para cifrar su clave K_B y enviar al nodo A el resultado $KU_A(K_B)$ (PIO). Por último, A usa su clave K_A para cifrar su almacén y enviar a B el cifrado $E_{KA}(Almacén_A)$ (P11).

Figura 8: Generador de secuencia cifrante basado en un registro de desplazamiento con polinomio de realimentación primitivo de coeficientes (c_L, c_{L-1},..., c_1) de menores valores no nulos, tales que el peso de dicho vector de coeficiente es el menor valor mayor que 0,07*L. Incluye una función de filtrado f de orden igual al número primo p más cercano a L/2, término lineal correspondiente a p, y número de términos de cada orden i = 1, 2,..., p igual a [L/i], La salida de dicho filtrado se décima según la salida del registro, y la salida decimada se introduce en un buffer de tamaño 4.

Figura 9: Formación de grupo reactivo generado *ad-hoc* a partir de la detección de un atasco.

Figura 10: Esquema representando las tres zonas geográficas definidas para la autenticación de datos llamadas zona de peligro (Z1), zona de incertidumbre (Z2) y zona de seguridad (Z3).

Figura 11: Representación gráfica de uso del cálculo de la velocidad a partir de la distancia s recorrida en un tiempo t por un nodo, permitiendo que el dispositivo recalcule automáticamente el tiempo t_e estimado para la ruta inicialmente recomendada y lo compare con el tiempo t_h inicialmente estimado para esa ruta, de forma que si $t_e >> t_h$, y existe una ruta alternativa con tiempo estimado $t_a << t_e$, el dispositivo recomienda esta ruta al conductor.

Modo de realización de la invención

Aunque el planteamiento general de la invención puede ser usado en diferentes aplicaciones de las VANETs, los análisis llevados a cabo y la realización concreta descrita como modo de realización están centrados en el objetivo de la reducción de atascos en la carretera.

En este caso se utilizan teléfonos móviles como dispositivos móviles, de forma que el nodo que representa al vehículo dentro de la red vehicular en cada momento es el teléfono móvil del pasajero asociado en primer lugar al dispositivo manos libres del vehículo. Esta última suposición evita la posibilidad de que en un vehículo sean varios los dispositivos de sus pasajeros que puedan estar figurando en la VANET, ya que esto conduciría a conclusiones erróneas sobre densidad de vehículos en la carretera. Además, en el momento de sincronización del teléfono móvil como primer aparato asociado al dispositivo manos libres, el teléfono móvil modifica automáticamente de “modo peatón” a “modo vehículo”. En “modo peatón” el teléfono móvil únicamente tiene activos los componentes C2, C3, C4, C5 y C6, que le permiten actualizar su almacén de claves.

Para usar esta invención el usuario no tiene que realizar ninguna acción específica mientras conduce. Antes de poner en marcha el vehículo, introduce en el dispositivo su destino y preferencia de ruta. Nuestra propuesta implica

que el dispositivo recibe y envía información automáticamente, usando únicamente la red vehicular y sin necesidad de requerir la colaboración del conductor en ningún momento (ver Figura 5). Cuando el dispositivo detecta que el vehículo está circulando a una velocidad anormal con respecto a la vía, genera un aviso y lo envía a todos sus vecinos vía broadcast. Con las informaciones recibidas, el dispositivo recalcula automáticamente la ruta recomendada y se la sugiere al conductor.

A continuación se describen varios conceptos y algoritmos propuestos como realización preferida de la invención, con el objetivo concreto mencionado.

Para el módulo C1 se propone como realización particular, que la clave pública de identidad se genere como valor decimal de la representación binaria correspondiente a la submatriz triangular superior de la matriz simétrica de adyacencia que contiene los elementos correspondientes a un circuito hamiltoniano en un grafo (ver Figura 6).

En el módulo C3 proponemos en esta realización específica, que el seudónimo variable de cada nodo sea el hash del listado de IDs de los nodos presentes en su almacén de claves públicas en ese momento. Dado que dicho almacén va variando, el seudónimo también varía. Además así se puede realizar la comprobación de que los IDs enviados en el primer paso de la autenticación se corresponden con el hash enviado en el beacon correspondiente.

En el módulo C4 proponemos para esta realización concreta, según se muestra en la Figura 7, que un nodo B que desee establecer contacto con un nodo A en primer lugar le solicite el listado de IDs de su almacén en ese momento, compruebe coincidencia de su hash con el seudónimo enviado por A en su beacon, y le responda indicando una clave X presente en la intersección de ambos almacenes. Luego, la demostración de conocimiento nulo mutua se realiza sobre la clave pública X de manera que cada nodo construye a partir de dicha clave, considerándola como circuito hamiltoniano, un grafo G en el que X sea solución al problema difícil del circuito hamiltoniano, y lo envía al otro nodo. Después se realizan al menos dos iteraciones de la demostración de forma que en un primer paso cada nodo envía al otro como testigo de compromiso un grafo isomorfo GI al grafo previamente enviado. A continuación cada nodo envía al otro un reto aleatorio indicando si desea recibir del otro nodo el isomorfismo entre ambos grafos o bien un circuito hamiltoniano en el grafo isomorfo. Al finalizar la demostración de conocimiento nulo, ambos nodos saben que comparten la clave pública X, que usan para cifrar mediante el cifrado simétrico descrito más adelante, y enviar al otro nodo su propia clave pública de identidad. Después se intercambian sus claves secretas temporales cifradas con la clave pública del otro nodo y finalmente cada uno usa su propia clave secreta temporal para cifrar con el cifrado simétrico descrito a continuación, y enviar cifrado su almacén de claves, que es contrastado contra el seudónimo remitido en el beacon y el listado de IDs enviado en el primer paso de la autenticación.

Para la implementación del módulo C5 proponemos que se utilice el algoritmo de actualización de almacén descrito a continuación. En él cada nodo escoge para guardar en su almacén aquellos certificados de claves públicas de los nodos que más certificados válidos han emitido o recibido, ya que con ello maximizan la probabilidad de intersección entre almacenes, necesaria en el módulo C4. Los certificados y nodos del almacén se tratan en dicho algoritmo respectivamente como aristas y vértices de un grafo.

Función Actualización_Almacén()
  Inicializar las estructuras de datos;
  u:=B;
  Para cada (u,ID) ∈ $Almacén_A \cup Almacén_B$
    Si grado_ponderado(ID)>máximo(grado_ponderado($Almacén_A \cup Almacén_B$)
      Si cardinal($Almacén_B$)<lím *ó*
      grado_ponderado(ID)>máximo(grado_ponderado($Almacén_B$))
        Añadir (u,ID) a $Almacén_B$;
        u:=ID;
      Fin si
    Fin si
  Fin para
Fin función

Para la implementación del módulo C6 proponemos que al nodo deshonesto, en lugar de borrar directamente su clave pública del almacén tras un comportamiento indebido, se refleje su conducta asignando en el almacén un peso negativo a las aristas correspondientes a certificados emitidos o recibidos por él, de forma que al recibir dichos certificados un peso negativo, el vértice dejará progresivamente de estar presente en los almacenes actualizados. Este esquema se combina en el algoritmo de actualización de almacenes con una asignación de pesos a aristas en el almacén, según el siguiente criterio: 2 para certificados emitidos o recibidos directamente por el nodo, 1 para el resto de certificados, -2 para certificados denunciados directamente por el nodo, y -1 para certificados denunciados por otros nodos.

Para su uso en el módulo C7, así como para el cifrado de clave secreta contemplado en el módulo C4 proponemos un cifrado simétrico eficiente. Dicha eficiencia es imprescindible ya que en su primer uso en el módulo C4 la longitud de la clave usada, al tratarse de una clave pública, es en general superior a la establecida como segura para los cifrados simétricos, mientras que en su segundo uso en C4, el almacén de claves en general es un fichero muy grande. También en el propio módulo C7 el fichero a cifrar conteniendo los datos de tráfico y carretera será en general muy grande. Así pues, proponemos como cifrado simétrico el cifrado en flujo binario usando como generador de secuencia cifrante el descrito en la Figura 8, que está basado en un registro de desplazamiento con polinomio de realimentación primitivo sobre GF(2), $1 + c_1x + c_2x^2 + ... + c_Lx^L$, de grado L igual a la longitud de la clave usada en cada momento, y alimentado con la semilla formada por dicha clave. El polinomio de realimentación del registro viene dado por el polinomio primitivo de menores coeficientes no nulos y número de dichos coeficientes dado por el menor número posible mayor que 0,07*L, para mejorar la eficiencia. El orden de la función de filtrado es el número primo p más cercano a L/2, para garantizar complejidad lineal grande. Dicha función incluye un término lineal correspondiente a su orden, además de un número de términos de cada orden i=1, 2,..., p dado por la parte entera de L/i, obtenidos multiplicando etapas sucesivas, para lograr seudoaleatoriedad y confusión. Para evitar ataques por correlación, la salida de dicho filtrado no lineal se decima irregularmente de manera que la salida del registro determina en cada momento si la correspondiente salida del filtrado se utiliza o se descarta. Finalmente, con objeto de garantizar una salida estable, se incluye un buffer de tamaño 4.

Como propuesta específica para la implementación del módulo C8 proponemos que la comprobación de coincidencias mediante agregación de datos se realice según un protocolo probabilístico basado en grupos reactivos, es decir, generados *ad-hoc* para producir un paquete agregado (ver Figura 9). Se distinguen para ello tres situaciones en las que se pueden encontrar los vehículos respecto a un incidente: Vehículos que son capaces de detectar un obstáculo o incidente en la carretera y se encargan de generar los correspondientes mensajes de advertencia; Vehículos que reciben los mensajes de advertencias y pueden confirmar que la información es cierta porque tienen contacto directo con el incidente; y Vehículos que reciben los mensajes de advertencia pero no son capaces de confirmar o desmentir dicha información dado que están fuera de rango. Por otra parte, dado que en la mayoría de casos la información generada en un determinado punto nos es de interés fuera de cierto radio de distancia respecto a dicho punto, se consideran tres zonas geográficas respecto a un incidente (ver Figura 10): Zona de Peligro (Z1) o zona central del área donde el peligro puede ser detectado directamente por el vehículo; Zona de incertidumbre (Z2) que rodea la zona de peligro y donde no es posible confirmar la información directamente pero donde la toma de decisiones debe ser rápida y eficaz porque en un corto periodo de tiempo el vehículo entrará en la zona de peligro; y Zona de Seguridad (Z3), donde los nodos se comportan siguiendo el paradigma de store-and-carry reuniendo evidencias acerca de un mismo peligro obtenidas mediante diferentes paquetes. Asimismo proponemos el establecimiento de grupos reactivos cuando se detecta un peligro, de manera que los vehículos cooperen formando grupos dentro de su rango, en la misma celda geográfica y generando información agregada evitando colisiones, retardos, sobrecargas en la red y repeticiones de información. Con la utilización de grupos pretendemos evitar que el número de paquetes generados en una zona de peligro para advertir de un problema crezca infinitamente, además de permitir la reducción del número de firmas contenidas en un paquete. El centro del área geográfica se corresponde con la localización del peligro existente y a partir de éste se generan los diferentes grupos. En cada grupo existe un líder encargado de construir el paquete y agregar las firmas de todos los vehículos de su grupo. La verificación de un mensaje de agregación solo se realiza en aquellos vehículos que son incapaces de verificar directamente la información, es decir, cuando un vehículo recibe un mensaje de advertencia sobre un incidente que está fuera de la cobertura de su antena y quiere confirmar la autenticidad del mensaje recibido. La verificación que realizan los vehículos depende del sentido de la marcha y de la zona geográfica en la que se encuentre. En la zona de incertidumbre, si un vehículo recibe un mensaje de agregación conteniendo n firmas, usa el registro de desplazamiento de longitud n definido en el módulo C7 alimentado con el primer bit de cada una de las firmas para generar n bits y verificar sólo las firmas indicadas por dicha salida. En la zona de seguridad, los vehículos comprueban una serie de firmas contenidas en el paquete tal como se describió en el caso anterior, pero además los vehículos podrán realizar otras verificaciones que les proporcionen mayor nivel de fiabilidad sobre la información recibida. Así, estando en esta zona, es posible recibir varios paquetes agregados correspondientes a un mismo peligro pero provenientes de diferentes grupos.

A los 8 módulos básicos del sistema descritos se añade para la realización concreta, un último módulo que posibilita la detección automática de condiciones anómalas de la carretera con el objeto de avisar con antelación a los conductores para evitar o reducir los atascos.

C9. *Cálculo de velocidad, condiciones anómalas de tráfico y rutas alternativas*

Este módulo usa la información recibida de un receptor de un sistema global de navegación por satélite. Es necesario para poder usar la red con objeto de ayudar a la conducción sin tener que instalar ningún tipo de infraestructura ni en el vehículo ni en la carretera (ver Figura 11).

REIVINDICACIONES

1. Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada que comprende:

- un módulo de generación de claves de identidad y de firma digital.

- un módulo que contenga arquitectura cliente/servidor con posibilidad de conexión a múltiples usuarios a la vez.

- un módulo de envío multicast y recepción inalámbrica de beacons con seudónimos variables.

- un módulo para autenticación mutua de nodos, con intercambio de claves públicas fijas, claves secretas temporales, y almacenes de claves públicas basado en un esquema interactivo de reto-respuesta.

- un módulo de actualización de los almacenes de claves públicas.

- un módulo de reputación de nodos, que borra de los almacenes a los nodos deshonestos, mediante el borrado de su clave pública de los almacenes de certificados.

- un módulo de intercambio cifrado de datos sobre elementos estáticos y dinámicos de la carretera, mediante la utilización de una clave secreta temporal del emisor.

- un módulo de autenticación de datos mediante la comprobación de coincidencias con otros mensajes recibidos mediante agregación de datos.

2. Sistema de comunicaciones seguras en una red *ad-hoc* vehicular espontánea y autogestionada según reivindicación 1 para la reducción de atascos en carretera donde:

- el módulo de generación de claves de identidad y de firma digital, se basa en la generación del valor decimal de la representación binaria correspondiente a la submatriz triangular superior de la matriz simétrica de adyacencia que contiene los elementos correspondientes a un circuito hamiltoniano en un grafo.

- el módulo de envío multicast y recepción inalámbrica de beacons con seudónimos variables se basa en el hash del listado de IDs de los nodos presentes en su almacén de claves públicas en ese momento.

- el módulo para autenticación mutua de nodos se basa en que un nodo B que desee establecer contacto con un nodo A en primer lugar le solicite el listado de IDs de su almacén en ese momento, compruebe coincidencia de su hash con el seudónimo enviado por A en su beacon, y le responda indicando una clave X presente en la intersección de ambos almacenes. Luego, se realiza una demostración de conocimiento nulo mutua sobre la clave pública X de manera que cada nodo construye a partir de dicha clave, considerándola como circuito hamiltoniano, un grafo G en el que X sea solución al problema difícil del circuito hamiltoniano, y lo envía al otro nodo. Después se realizan al menos dos iteraciones de la demostración de forma que en un primer paso cada nodo envía al otro como testigo de compromiso un grafo isomorfo GI al grafo previamente enviado. A continuación cada nodo envía al otro un reto aleatorio indicando si desea recibir del otro nodo el isomorfísmo entre ambos grafos o bien un circuito hamiltoniano en el grafo isomorfo. Al finalizar la demostración de conocimiento nulo, ambos nodos saben que comparten la clave pública X, que usan para cifrar mediante el cifrado simétrico descrito más adelante, y enviar al otro nodo su propia clave pública de identidad. Después se intercambian sus claves secretas temporales cifradas con la clave pública del otro nodo y finalmente cada uno usa su propia clave secreta temporal para cifrar con el cifrado simétrico descrito a continuación, y enviar cifrado su almacén de claves, que es contrastado contra el seudónimo remitido en el beacon y el listado de IDs enviado en el primer paso de la autenticación.

- el módulo de actualización de los almacenes de claves públicas se basa en utilizar un algoritmo en el cada nodo escoge para guardar en su almacén aquellos certificados de claves públicas de los nodos que más certificados válidos han emitido o recibido. Los certificados y nodos del almacén se tratan en dicho algoritmo respectivamente como aristas y vértices de un grafo.

- el módulo de reputación de nodos se basa en reflejar la conducta de un nodo deshonesto asignando en el almacén un peso negativo a las aristas correspondientes a certificados emitidos o recibidos por él, de forma que al recibir dichos certificados un peso negativo, el vértice dejará progresivamente de estar presente en los almacenes actualizados. Este esquema se combina en el algoritmo de actualización de almacenes con una asignación de pesos a aristas en el almacén, según el siguiente criterio: 2 para certificados emitidos o recibidos directamente por el nodo, 1 para el resto de certificados, -2 para certificados denunciados directamente por el nodo, y -1 para certificados denunciados por otros nodos.

- el módulo de intercambio cifrado de datos se basa en un cifrado en flujo binario usando como generador de secuencia cifrante un filtrado no lineal decimado y con buffer, de un registro de desplazamiento con polinomio de realimentación primitivo sobre GF(2) de grado L igual a la longitud de la clave usada en cada momento, alimentado

con la semilla formada por dicha clave, y con polinomio de realimentación dado por el polinomio primitivo de menores coeficientes no nulos y número de dichos coeficientes dado por el menor número posible mayor que 0,07*L. La función no lineal del filtrado tiene como orden el número primo p más cercano a L/2, incluye un término lineal correspondiente a su orden, además de un número de términos de cada orden i = 1, 2,..., p dado por la parte entera de L/i, obtenidos multiplicando etapas sucesivas. La salida de dicho filtrado no lineal se decima irregularmente de manera que la salida del registro determina en cada momento si la correspondiente salida del filtrado se utiliza o se descarta, introduciéndose en el primer caso en un buffer de tamaño 4.

- el módulo de autenticación de datos se basa en un esquema de agregación de datos basado en grupos reactivos en los que cada líder se encarga de construir el paquete y agregar las firmas de todos los vehículos de su grupo, y donde la verificación se realiza según un protocolo probabilístico que depende de la zona geográfica en la que se encuentre cada vehículo.

- se añade un módulo de detección automática de condiciones anómalas para el cálculo de velocidad, basado en la información recibida de un receptor de un sistema global de navegación por satélite.

Figura 1

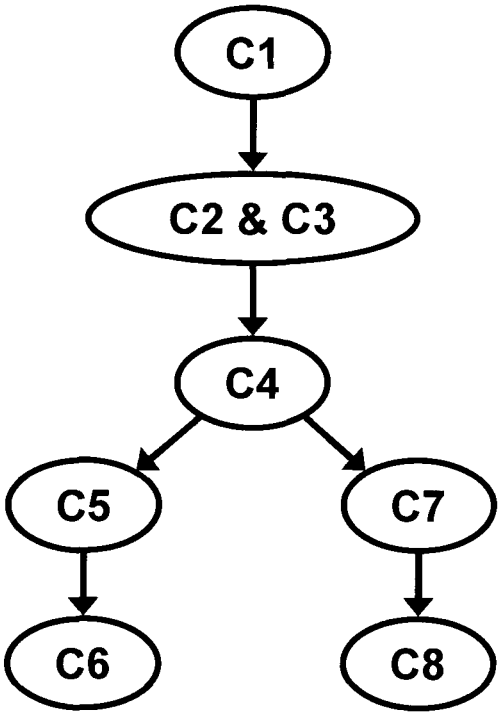


Figura 2

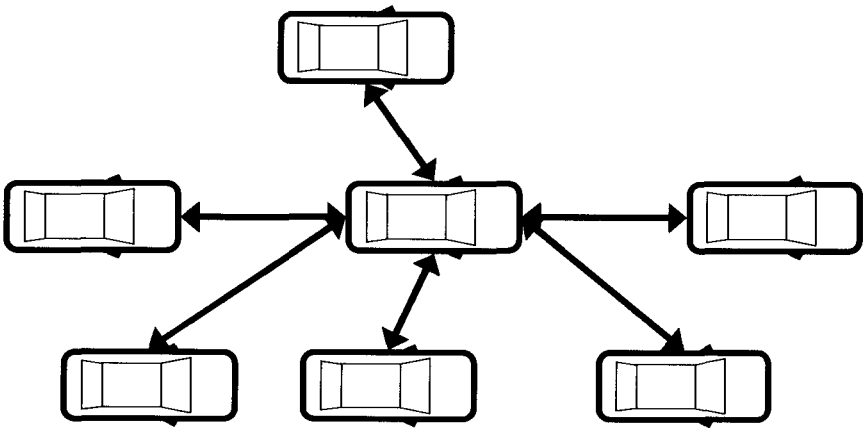


Figura 3

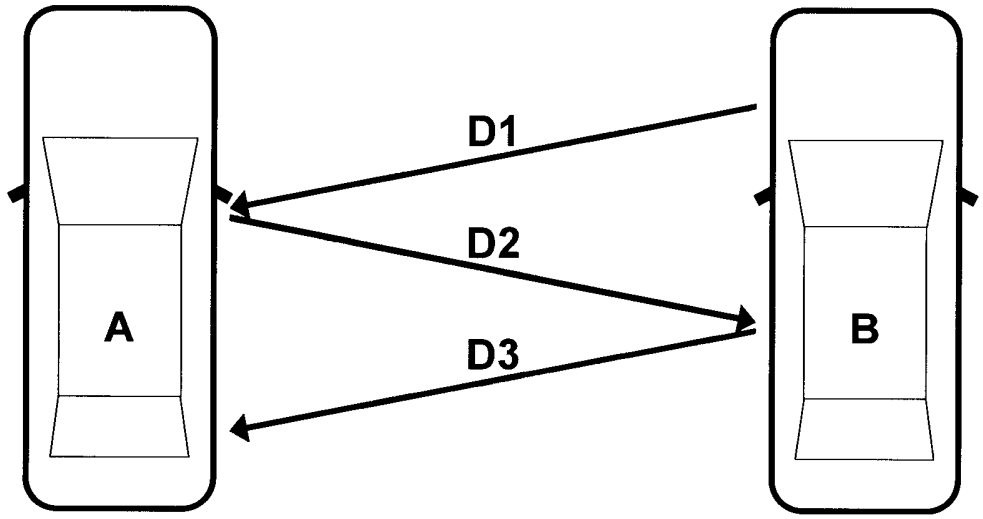


Figura 4

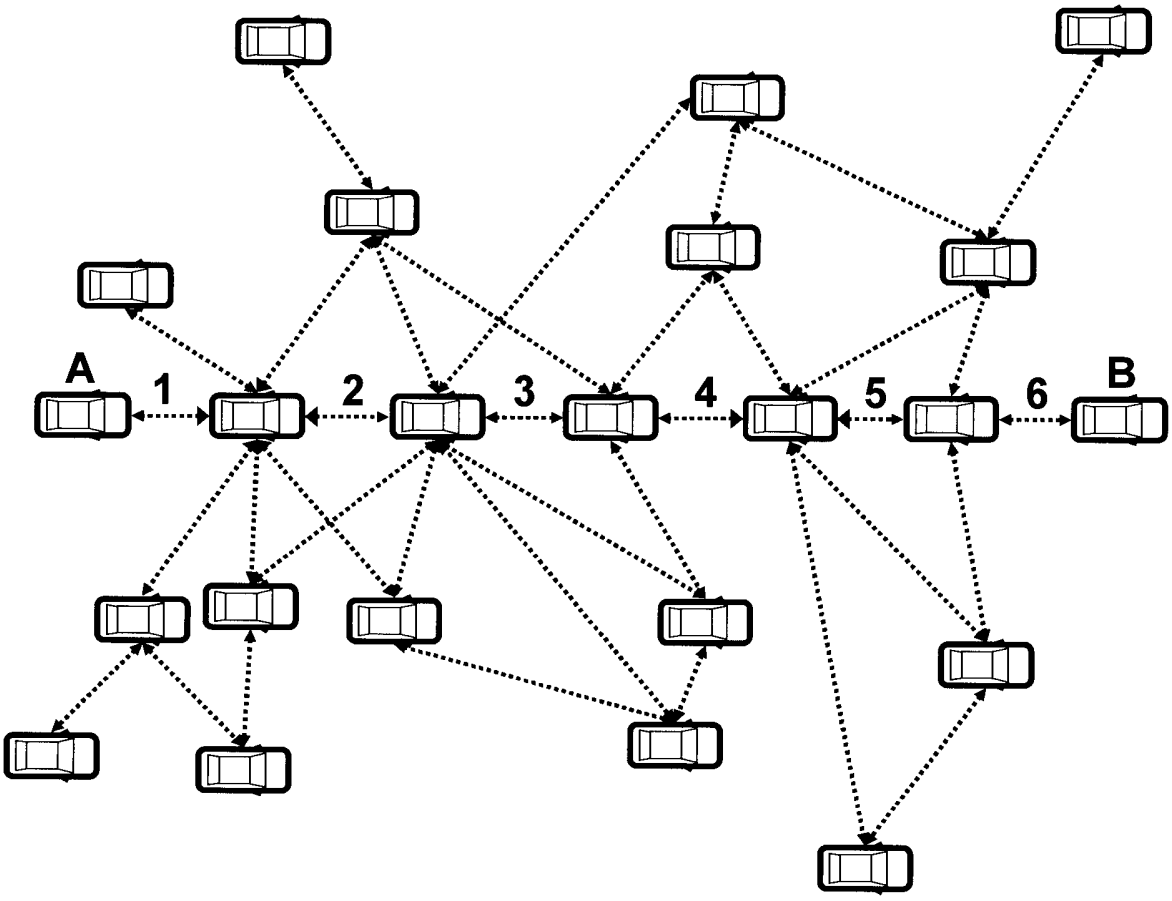


Figura 5

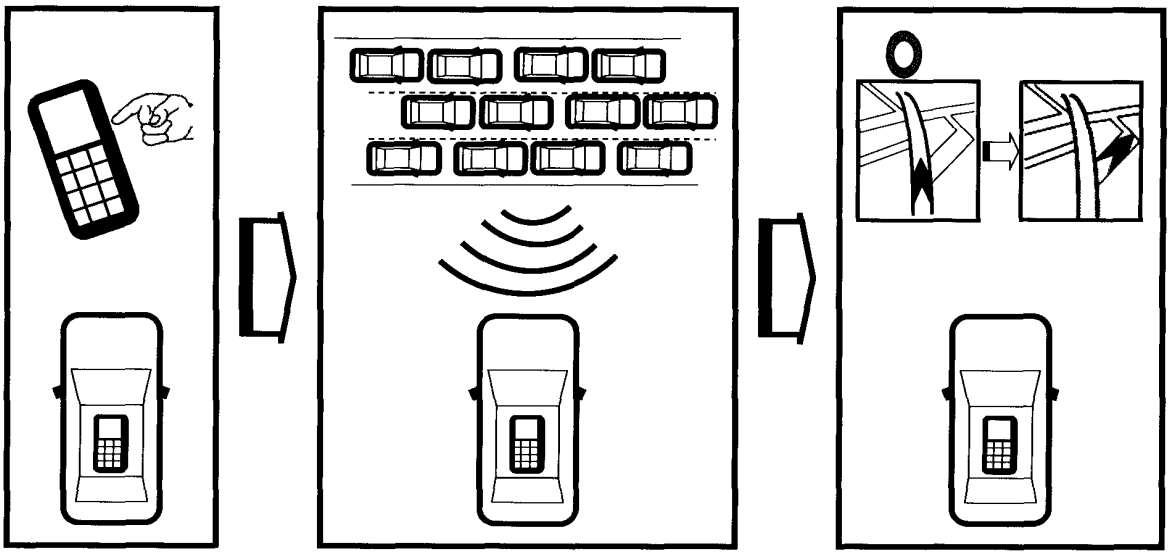
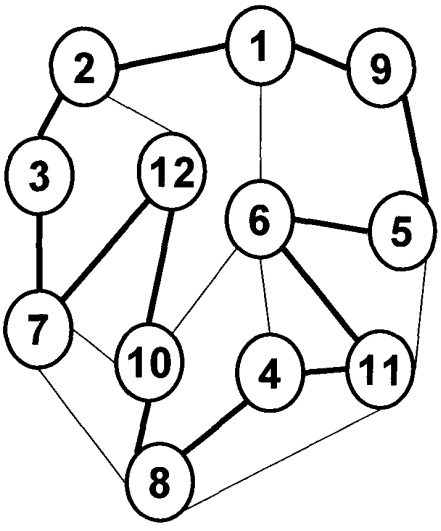


Figura 6



0	**1**	0	0	0	1	0	0	1	0	0	0
1	0	**1**	0	0	0	0	0	0	0	0	1
0	1	0	0	0	0	**1**	0	0	0	0	0
0	0	0	0	0	1	0	**1**	0	0	1	0
0	0	0	0	0	**1**	0	0	1	0	1	0
1	0	0	1	1	0	0	0	0	1	**1**	0
0	0	1	0	0	0	0	1	0	1	0	**1**
0	0	0	1	0	0	1	0	0	**1**	1	0
1	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	0	0	0	**1**
0	0	0	1	1	1	0	1	0	0	0	0
0	1	0	0	0	0	1	0	0	1	0	0

KU_{ID}: 1000000000010000000000001000000001000010000000000100000101000000010

Figura 7

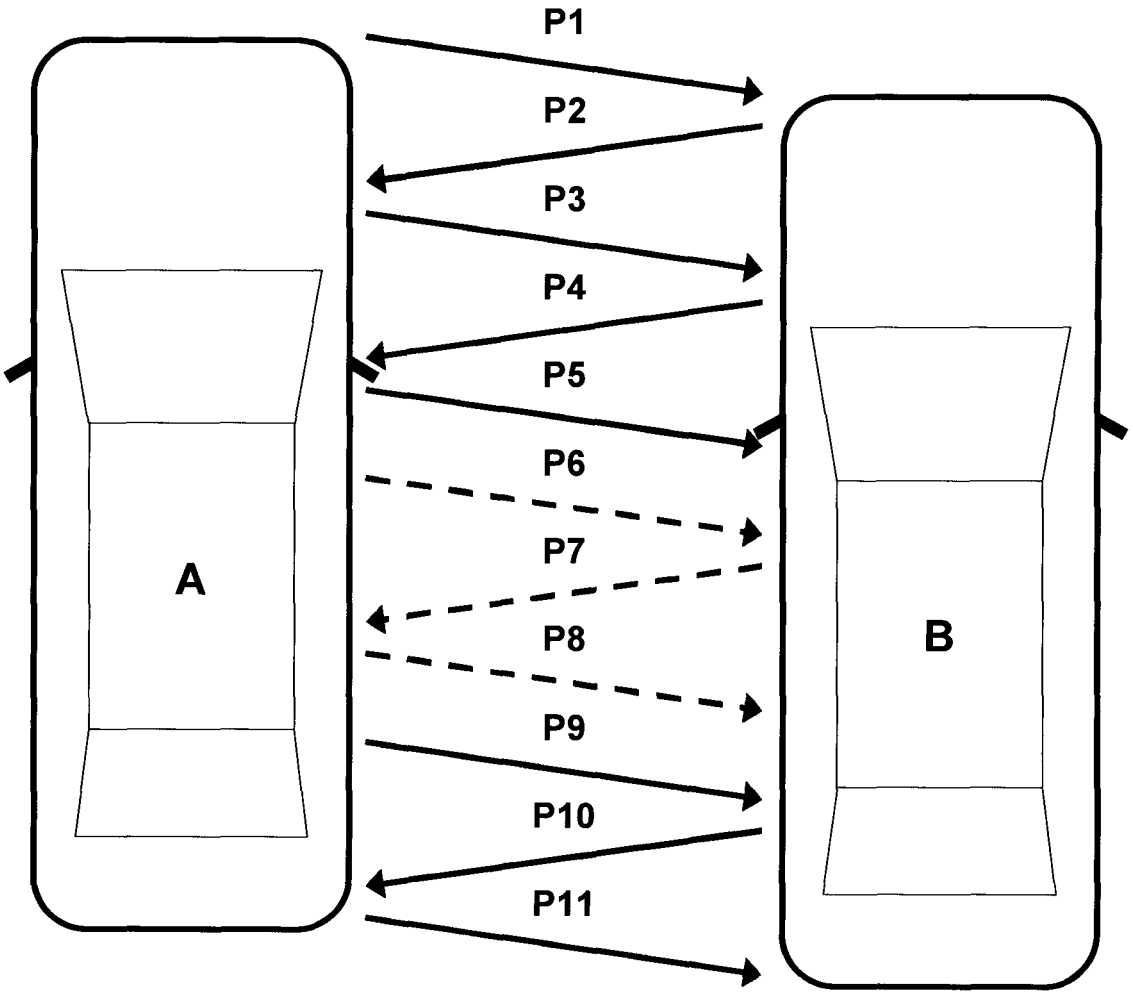


Figura 8

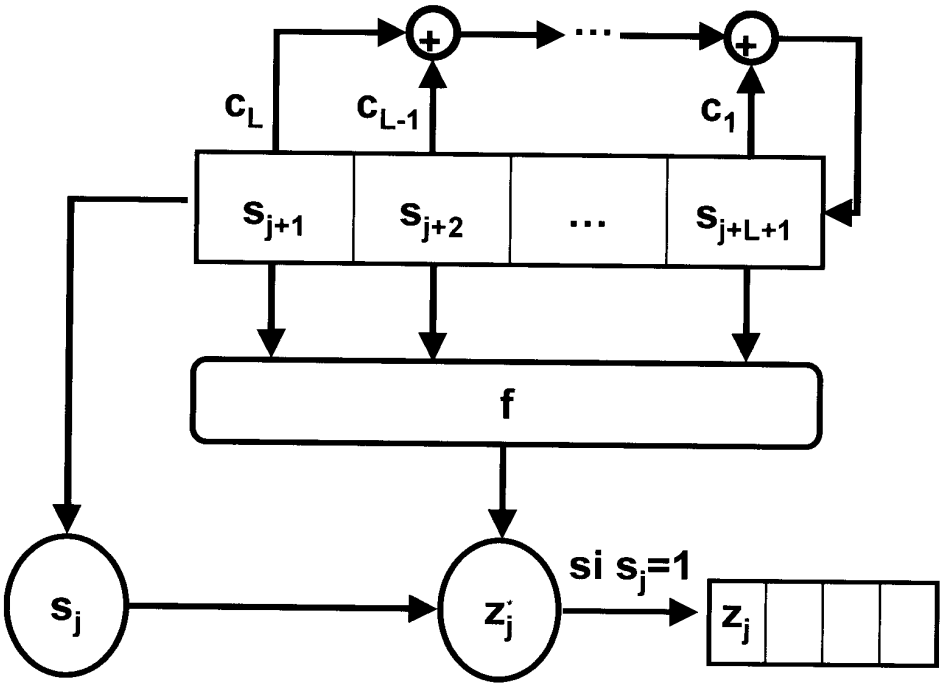


Figura 9

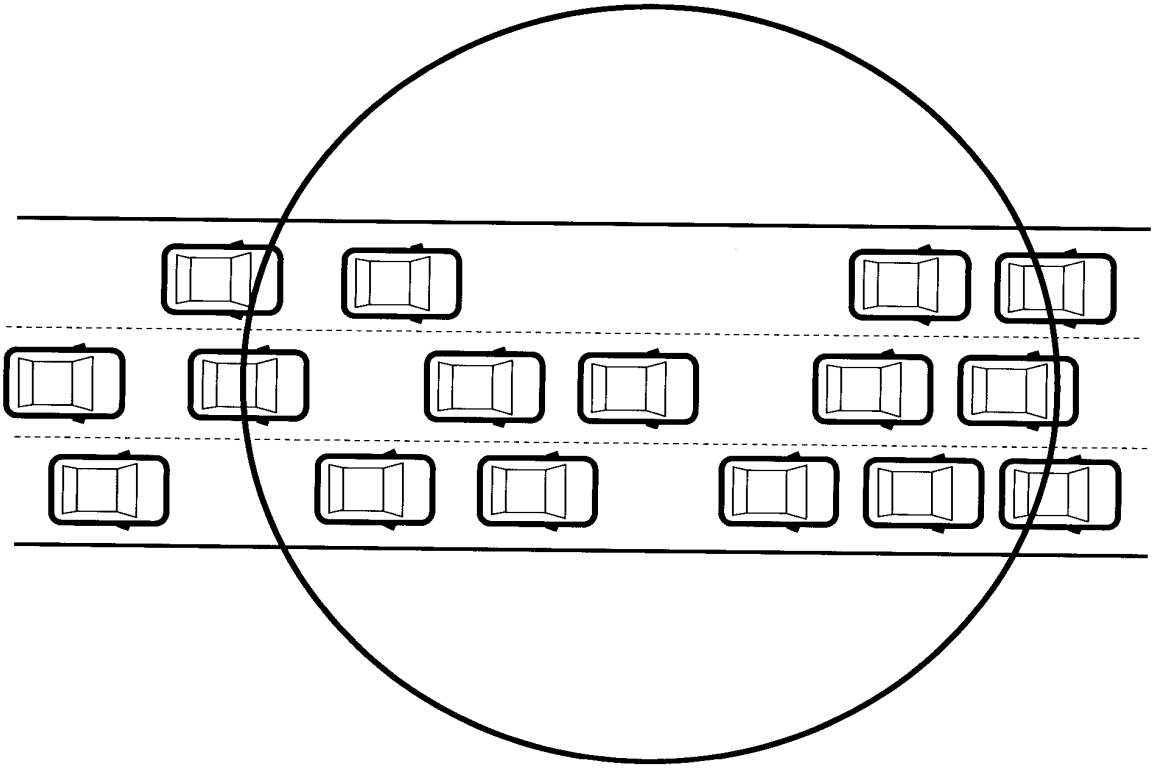


Figura 10

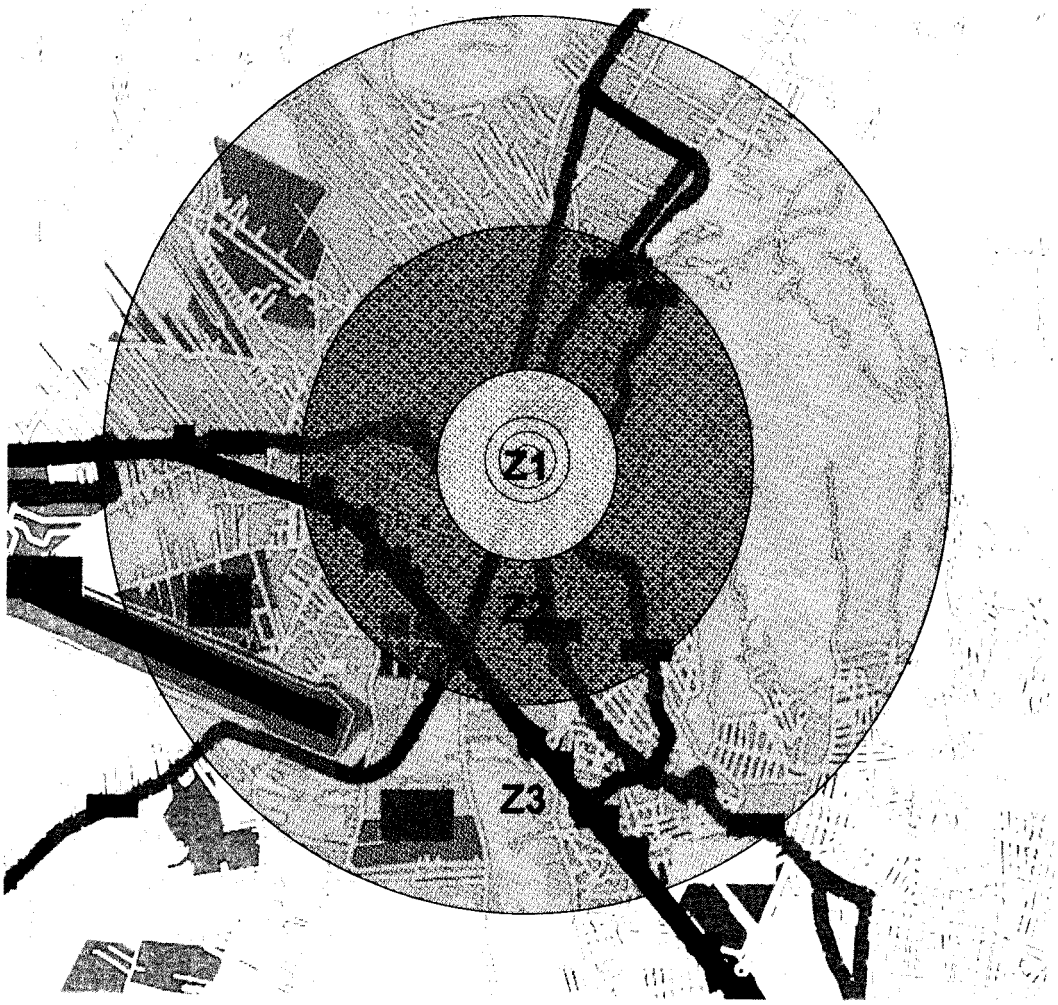
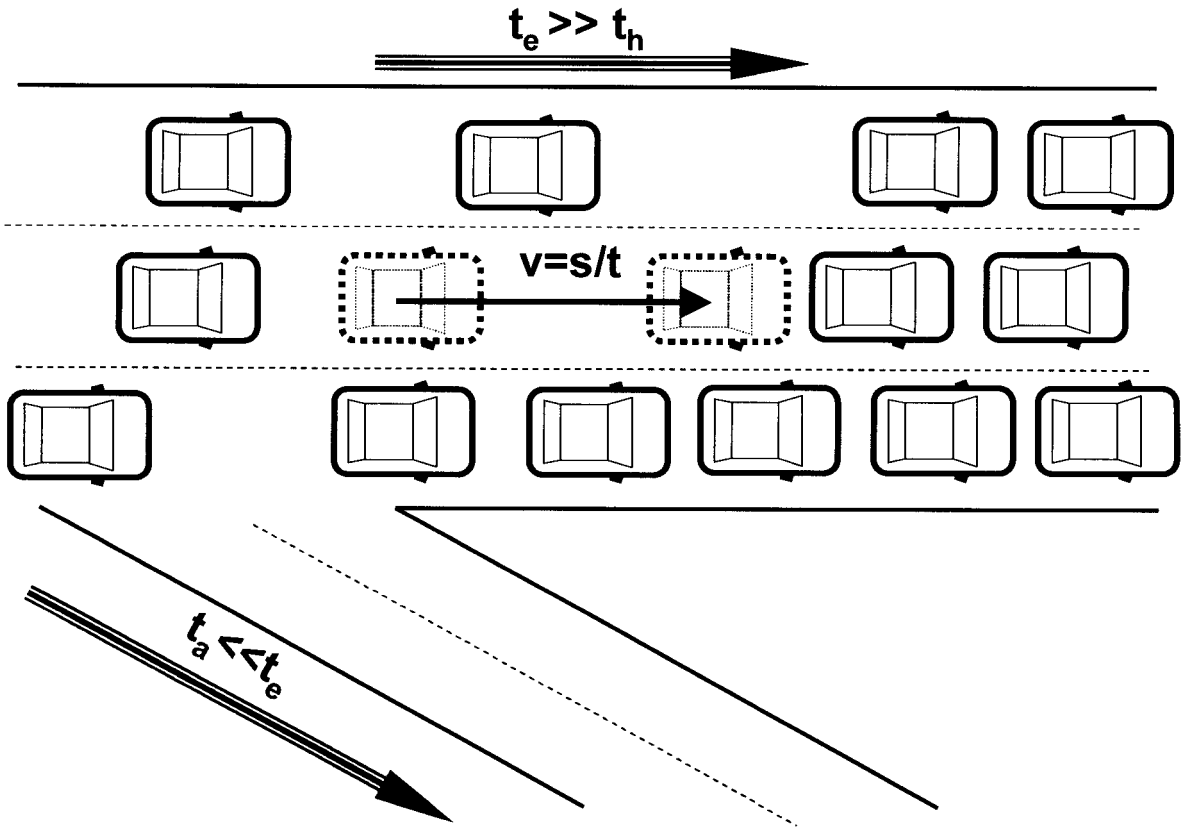


Figura 11



OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201000865

(22) Fecha de presentación de la solicitud: 29.06.2010

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W12/00*** (2009.01)
H04W84/18 (2009.01)

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
Y	CAPKUN et al. "Self-organized public-key management for mobile ad hoc networks". IEEE Transactions on Mobile Computing (2003). Vol 2 Issue 1 páginas 52-64. IEEE Piscataway, NJ, USA. 31.03.2003. ISSN 1536-1233. Todo el documento.	1
A		2
Y	RAYA et al. "Efficient Secure Aggregation in VANETs". Proceedings of the 3rd international workshop on Vehicular ad hoc networks 2006 páginas 67-75. 31.12.2006. ISBN: 1-59593-540-1. Todo el documento.	1
A		2
A	"Pretty Good Privacy". Artículo Wikipedia. Documento recuperado de internet http://es.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=38143026 [recuperado el 02.12.2011]. 18.06.2010. Todo el documento.	1-2
A	CABALLERO-GIL et al. "Self-organized authentication architecture for Mobile Ad-hoc Networks" International Symposium on 6th Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008, páginas 217-224. IEEE Piscataway, NJ, USA. 01.08.2008. ISBN 978-963-9799-18-9. Todo el documento.	1-2

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
04.01.2012	M. Rivas Sáiz	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04W, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 04.01.2012

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-2	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	2	**SI**
	Reivindicaciones	1	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	CAPKUN et al. "Self-organized public-key management for mobile ad hoc networks". IEEE Transactions on Mobile Computing (2003). Vol 2 Issue 1 páginas 52-64. IEEE Piscataway, NJ, USA. 31.03.2003. ISSN 1536-1233. Todo el documento.	31.03.2003
D02	RAYA et al. "Efficient Secure Aggregation in VANETs". Proceedings of the 3rd international workshop on Vehicular ad hoc networks 2006 páginas 67-75. 31.12.2006. ISBN: 1-59593-540-1. Todo el documento.	31.12.2005
D03	"Pretty Good Privacy". Artículo Wikipedia. Documento recuperado de internet http://es.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=38143026 [recuperado el 02.12.2011]. 18.06.2010. Todo el documento.	02.12.2011

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

El documento D01 se considera el más próximo del estado de la técnica a la invención solicitada.
Con relación a la reivindicación 1, D01 describe un sistema de comunicaciones seguras en una red ad-hoc móvil espontanea y autogestionada (resumen) que comprende:

-un módulo de generación de claves de identidad y de firma digital (epígrafe 3.1);

-un módulo que contenga arquitectura cliente/servidor con posibilidad de conexión a múltiples usuarios a la vez. Este módulo está implícito en el mismo funcionamiento de la red móvil tal como se indica en la figura 1;

-un módulo de envío multicast y recepción inalámbrica de beacons con seudónimos variables. De manera concreta, en el epígrafe 3.2 D01 describe que un nodo realiza un envío multicast de los valores hash de los certificados de su subgrafo que son variables.
-un módulo para autenticación mutua de nodos; En D01 describe una autenticación mutua de módulos con claves públicas/privadas y almacenes. En la reivindicación 1 este módulo también menciona claves secretas temporales y un esquema interactivo de reto respuesta pero está descrito como una yuxtaposición de elementos sin indicar la interacción entre ellos. El intercambio de claves secretas temporales y la utilización de un esquema interactivo de reto respuesta son técnicas conocidas y ampliamente utilizadas para la autenticación mutua de nodos. Dado que en la reivindicación 1 no se indica de forma funcional cómo es la interacción entre estos elementos, la yuxtaposición de estas técnicas, ampliamente conocidas, no dotan a la reivindicación de actividad inventiva.

-un módulo de actualización de los almacenes de claves públicas (epígrafe 3.3);

-un módulo de reputación de nodos, que borra de los almacenes a los nodos deshonestos, mediante el borrado de su clave publica de los almacenes de certificados (epígrafe 3.4);

El documento D01, describe con detalle la autenticación entre nodos de una red MANET sin embargo no describe el intercambio de datos de manera cifrada. El cifrado de datos es una técnica ampliamente conocida para conseguir confidencialidad. Por ejemplo, el sistema PGP (Pretty Good Privacy, privacidad bastante buena) mencionado en el documento D03, es un sistema ampliamente conocido que utiliza una clave simétrica de sesión para encriptar el mensaje. Por consiguiente se considera que incluir un módulo de intercambio cifrado mediante clave simétrico es una técnica conocida que su inclusión en la reivindicación 1 no dota a dicha reivindicación de actividad inventiva.

D01 no menciona un módulo de autenticación de datos mediante comprobación de coincidencias con otros mensajes recibidos mediante agregación de datos. Los efectos técnicos de esta diferencia son proteger contra ataques que de distribución de contenidos falsos y evitar la saturación de la red debido al envío de mensajes con el mismo contenido. El problema técnico es proteger contra ataques que de distribución de contenidos falsos y además, evitar la saturación de la red debido al envío de mensajes con el mismo contenido. D01 no enuncia este problema.

El documento D02 describe un sistema de seguridad en una red VANET basado en la agregación de datos y la autenticación de los mismos. Tal como se indica en el epígrafe 4.1 D02 divulga tres sistemas de combinación de firma digitales para autenticar datos agregados.

Por tanto, un experto en la materia combinaría las características mencionadas en D01 con el módulo de agregación de datos de D02 para obtener la reivindicación 1 sin ayuda de la actividad inventiva. Por tanto, se concluye que la reivindicación 1 no implica actividad inventiva (Artículo 8 LP.).

Los documentos D01 y D02 no describen el funcionamiento de los módulos de autenticación mutua de los nodos ni el módulo de intercambio cifrado de datos descrito en la reivindicación 2. Por tanto se concluye que la reivindicación 2 es nueva e implica actividad inventiva (Artículos 6 y 8 LP.).