Conexión segura entre dispositivos móviles para la asistencia a la conducción

F. Martín-Fernández, P. Caballero-Gil, C. Caballero-Gil, J. Molina-Gil
Departamento de Estadística, Investigación Operativa y Computación,
Universidad de la Laguna
Email: fmartinfdez@gmail.com, {pcaballe, ccabgil, jmmolina}@ull.es

***Resumen*—Este trabajo describe la implementación de una herramienta para la asistencia a la conducción, llamada VAiPho (VANET in Phones), que permite crear la primera red vehicular real utilizando únicamente teléfonos móviles, siguiendo la idea de la interconexión entre objetos propuesta en la Internet de las Cosas. Concretamente se propone el desarrollo de VAiPho para diversas plataformas, centrándose en el sistema operativo Symbian, de forma que permite no sólo la detección automática de los eventos que ocurren en las carreteras en tiempo real, sino también las comunicaciones seguras entre vehículos para difundir avisos sobre dichos eventos. De hecho, la propuesta incluye la implementación de un esquema de autenticación fuerte basado en algoritmos criptográficos y confianza distribuida entre los usuarios. Por otra parte, la detección de eventos se realiza de manera óptima para saber con certeza dónde y cuándo se da una determinada condición de tráfico, como un atasco o un aparcamiento libre. Se incluye para ello un esquema de agregación de datos que permite corroborar con otros usuarios que un evento es real, y así evitar posibles mensajes erróneos o malintencionados.**

I. Introducción

Si nos preguntaran sobre nuestra idílica visión de un futuro cercano, muchos contestaríamos en base a los avances tecnológicos. Soñar con un mundo totalmente conectado en el que los objetos sean lo suficientemente inteligentes como para sentir el entorno, interactuar con él y compartir información, ya no parece tan descabellado gracias a conceptos como la Internet de las Cosas, que es un tema en auge en los últimos tiempos. Su visión es muy simple: si todos los electrodomésticos, vehículos y objetos en general, estuvieran equipados con dispositivos de identificación y se pudieran interconectar, la vida cotidiana en nuestro planeta sufriría una transformación. Por ejemplo, ya no existirían productos fuera de stock o perdidos, lo que sería de gran utilidad en logística; y los vehículos estarían localizados en todo momento, por lo que se podría gestionar el tráfico de una forma precisa y exacta, resolviendo los problemas de atascos y aparcamientos.

La Internet de las Cosas tiene como uno de los temas más incandescentes, y sobre el que muchos divagan en su visión futurista, la gestión inteligente del tráfico, necesaria tanto por las consecuencias en las pérdidas de vidas, como por su negativo efecto en la economía y en el medioambiente. Una medida de solución que ha sido propuesta en la bibliografía científica es la implantación de redes vehiculares o VANETs (Vehicular Ad-hoc NETworks), en las que los vehículos se comunican entre sí para prevenir y/o evitar circunstancias adversas en las carreteras y lograr una gestión más eficiente del tráfico. Dichas redes son una componente significativa de los Sistemas Inteligentes de Transporte o ITS (Intelligent Transportation Systems), que proponen un conjunto de soluciones tecnológicas diseñadas para mejorar la eficiencia y seguridad del transporte terrestre. Entre los muchos paradigmas de la Internet de las Cosas, este trabajo se centrará en lo concerniente a las VANETs.

Las VANETs pueden verse como una extensión de las redes móviles ad-hoc o MANETs (Mobile Ad-hoc NETworks) con una tecnología que utiliza vehículos en movimiento como nodos de la red. De esta forma se convierte a todos los vehículos participantes en routers o nodos que son capaces de comunicar información entre diversos vehículos vecinos y el sistema de tráfico.

Las primeras propuestas sobre redes ad-hoc vehiculares se publicaron en la década de los 70, aunque el término VANET fue acuñado en el año 2004 durante el primer encuentro internacional sobre redes ad-hoc vehiculares [6]. Desde entonces, muchos investigadores han tratado diversos tópicos relacionados con las VANETs, como autenticación, cooperación, cifrado, implementación, aplicaciones, etc. con el objetivo de diseñar propuestas seguras y eficientes. Sin embargo, es de destacar que la implantación real de las VANETs, tal como ha sido propuesta hasta ahora por la mayor parte de los investigadores, conllevaría un esfuerzo económico muy elevado, lo que ha frenado su desarrollo.

Uno de los principales requisitos de cualquier VANET es que los usuarios legítimos sean los únicos que puedan acceder a ella, una vez autenticados. La privacidad de los datos es también fundamental para garantizar al usuario que puede utilizar este tipo de tecnología sin miedo a seguimientos o usos de su información. En cuanto a la autenticación en VANETs se han propuesto diversas soluciones basadas en distintos algoritmos criptográficos. Una de las propuestas más habituales es el uso de infraestructuras de clave pública (PKI) [11] [12] [13] [19], si bien dichos esquemas tienen una gran complejidad computacional, lo que conlleva mucha ineficiencia si se aplica en grandes redes [1] [17]. En las soluciones clásicas basadas en PKI surge además el problema de la sobrecarga de comunicaciones y cómputo si el número de nodos excluidos de la red es grande, ya que implica gestionar grandes listas de revocación de certificados. En [10] ofrecen una solución basada en la pre-distribución de claves [3], y la generación de

claves de grupo. Otras soluciones basadas en el anonimato, y en particular en el concepto de pseudónimo [18], tratan de subsanar el problema de que en los actuales esquemas basados en el modelo cliente servidor, sólo los clientes se preocupan por la privacidad de los datos, ya que el servidor normalmente no tiene en cuenta este aspecto. Uno de los peores ataques que pueden recibir este tipo de redes es que usuarios legítimos pero con mala intención transmitan mensajes sobre eventos que no están sucediendo o bien mensajes erróneos. Algunas propuestas proponen para ello el uso regular de firmas digitales de todos los mensajes transmitidos [2] [14] [15] [16] para permitir el seguimiento de los vehículos maliciosos. Otro de los problemas que hay que considerar en grandes redes es la necesidad de fomento de la cooperación, que en el caso de las VANETs es más complejo ya que los nodos son transitorios y las comunicaciones son inalámbricas. Trabajos como [7] proponen la gestión de la información en grupos de vehículos, de manera que un vehículo sea el que tenga el acceso al recurso, y los demás accedan a él a través suyo.

Este trabajo describe la implementación de una propuesta novedosa para instaurar una red vehicular ad-hoc, poniendo énfasis en la seguridad de las comunicaciones entre vehículos, en cualquier punto del planeta a través de una aplicación para móviles denominada VAiPho. Se detalla el desarrollo llevado a cabo para un primer prototipo en la plataforma móvil Symbian, denotando que dicha aplicación está en avanzado estado de desarrollo y que cuenta con prototipos totalmente funcionales y acabados en diversas plataformas como son Windows Mobile, Android o la propia Symbian.

La propuesta aquí analizada propone una solución innovadora que incorpora algunas de las ideas mencionadas en una VANET desplegada, utilizando sólo dispositivos móviles como los teléfonos inteligentes que ya existen, con capacidad para albergar tecnologías tan simples y cotidianas como Bluetooth, GPS o WiFi. Este trabajo se organiza de forma que las secciones II y III describen respectivamente los diferentes módulos e interfaces de la aplicación, y la sección IV cierra el trabajo con algunas conclusiones y trabajos futuros.

II. Implementación y desarrollo

La aplicación VAiPho [4] [5] [8] [9] es una herramienta de software para teléfonos móviles que proporciona asistencia a la conducción mediante anuncios sobre diferentes tipos de eventos en la carretera tales como atascos y aparcamientos libres, cuyo conocimiento puede ser de utilidad para los conductores. Los eventos son detectados, transmitidos y retransmitidos automáticamente por el dispositivo. Además, una vez recibidos y comprobados determinados anuncios, VAiPho informa al conductor sobre los eventos a través de mensajes sonoros, lo que permite que centre toda su atención en la conducción. En este trabajo, cada vehículo que contenga un teléfono móvil ejecutando VAiPho se considera un nodo de la VANET.

Para realizar las primeras implementaciones de VAiPho se seleccionaron varias plataformas móviles, siguiendo una estructura en módulos como se puede observar en la figura 1. En esta ponencia se expone en particular la llevada a cabo para el sistema operativo de la compañía finlandesa Nokia, denominado Symbian, aunque cabe destacar que el desarrollo de VAiPho también ha sido desarrollado para Android (de Google Inc.), y para Windows Phone (de Microsoft Corp.).

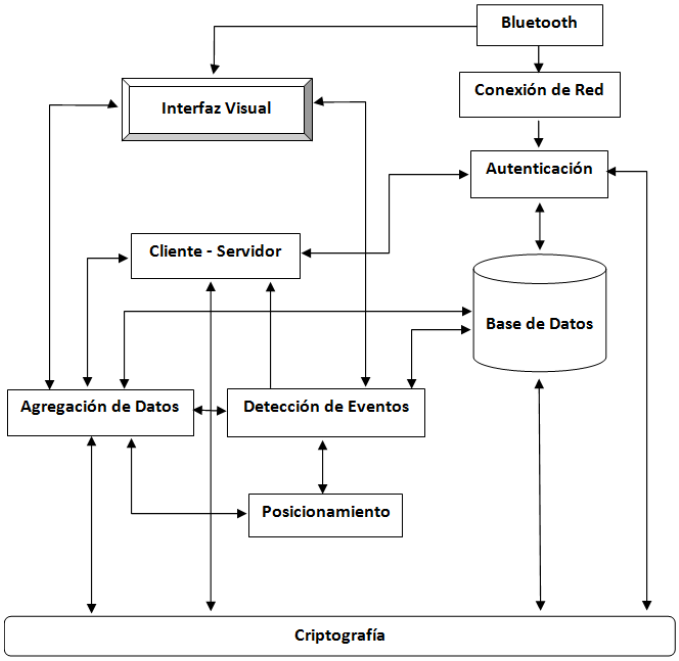

Figura 1. Relación entre los módulos de VAiPho para Symbian

II-A. Módulo de Conexión de Red

El módulo más esencial y básico que tiene VAiPho es el de la conexión de red, para poder comunicar los eventos de tráfico. Al tratarse de una VANET, la red usada es de tipo ad-hoc y creada espontáneamente por la aplicación. En particular, el primer terminal móvil que ejecute VAiPho en un determinado lugar crea la red ad-hoc, ya que esta red no existe previamente. Sucesivos usuarios que usen VAiPho en este lugar mientras exista la red creada, se conectarán directamente a esta red sin necesidad de crear una nueva. De hecho, si el primer usuario creador de la red, la abandona porque deja de utilizar la aplicación, la red ad-hoc seguirá existiendo mientras alguno de los usuarios que se hubieran conectado a ella siga conectado, ya que cada usuario tiene la información necesaria para seguir transmitiendo datos a través de ella.

Dado que la red ad-hoc que se crea debe tener un nombre común para que todos los terminales puedan reconocerla, se decidió que dicho nombre fuese el mismo que tiene la aplicación: 'vaipho'. De esta manera, la aplicación puede reconocer si existe la red ad-hoc con nombre 'vaipho'y conectarse en caso positivo, o bien crearla en caso contrario. Con esto ya es suficiente para que la aplicación pueda conectarse adecuadamente a la red ad-hoc con la que trabajará en su ciclo de vida.

Se ha hecho un análisis de tiempos de conexión a la red vaipho, distinguiendo cuándo había que crearla de cuándo

ya existía, y diferenciando si la aplicación estaba corriendo en el terminal móvil o bien en el simulador del entorno de desarrollo. Como se observa en la Tabla 1, los tiempos que tarda en realizar estas acciones el simulador son muy pequeños debido a la capacidad de cómputo del ordenador. Sin embargo, en un terminal móvil real estos tiempos son mayores y por tanto han tenido que ser considerados durante la implementación real de vaipho.

	Con la red ya creada	**Creando la red**
Simulador	menor que 1	entre 1 y 3
Terminal móvil	entre 15 y 20	entre 40 y 60

Tabla 1. Tiempo (en segundos) de conexión a la red

II-B. Módulo Cliente-Servidor

Un módulo de comunicaciones cifradas siguiendo la arquitectura del modelo cliente servidor, es otra parte importante de la aplicación ya que en VAiPho es imprescindible que la aplicación pueda servir tanto de cliente como de servidor. Esta peculiaridad se logra creando un hilo de ejecución que maneje el cliente y otro hilo de ejecución que maneje el servidor. De esta manera la aplicación puede enviar paquetes a la red mediante el cliente, y estar continuamente escuchando los paquetes que pueda recibir para tratarlos por el servidor.

Como configuración idónea para realizar los envíos y recepciones en la red se usa un protocolo a nivel de transporte basado en el intercambio de datagramas (paquetes de datos), conocido como UDP. El protocolo UDP permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. No tiene confirmación ni control de flujo por lo que los paquetes pueden adelantarse unos a otros, y no se sabe si ha llegado correctamente ya que no hay confirmación de entrega o recepción. Su uso habitual es para protocolos en los que el intercambio de paquetes de conexión/desconexión es mayor, o que no son rentables con respecto a la información transmitida y la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tienen en estos casos. Este protocolo utiliza un puerto para enviar y escuchar los datos en la red.

El módulo cliente es el encargado de enviar los datos pertinentes a la red, envío que se puede realizar a una dirección concreta de la red o bien por el contrario, a toda la red en modo broadcast. El módulo servidor es el encargado de recibir todos los paquetes que lleguen directa o indirectamente a la aplicación a través de la red, para procesarlos adecuadamente.

II-C. Módulo de Autenticación

Otra cuestión fundamental abordada en el diseño e implementación de VAiPho es la autenticación mutua de los nodos en la VANET. Para poder utilizar adecuadamente VAiPho, es necesario que los usuarios de la red sean de confianza y no fraudulentos. El algoritmo utiliza un intercambio de mensajes cifrados para verificar la identidad del otro usuario y así poder discernir si es confiable o no.

Se estableció que cada usuario, aparte de su identificador único asociado a su clave pública, use para anunciarse en la red un PSEUdónimo (PSEU) variable, ya que de esta manera se logra asociar dicho pseudónimo unívocamente a cada usuario y a la vez dicho pseudónimo sirve como alias para darse a conocer al resto sin poner en peligro su privacidad gracias a que no es fijo. Además se utiliza durante la autenticación un algoritmo basado en un esquema interactivo de reto-respuesta, que se detalla a continuación.

El algoritmo incluye una serie de mensajes que se intercambian dos terminales móviles. Se distinguen 3 tipos de mensajes: D (Descubrimiento), Z (Conocimiento) y E (Intercambio de información). El proceso de la autenticación comienza con la recepción de un mensaje o beacon que los smartphones envían periódicamente en modo broadcast a la red para anunciar su presencia.

Una usuaria A (Alice) recibe de un usuario B (Bob), el beacon mencionado, y si no se han autenticado previamente, empiezan el proceso de autenticación. La usuaria A responde este primer mensaje con un mensaje de tipo D1, que incluye el hash de cada uno de los identificadores de los usuarios que haya autenticado hasta entonces. Esta información sirve para comprobar si entre A y B existe algún usuario autenticado por ambos, que aporte confianza a dicha autenticación. Si no se diera esta circunstancia, la autenticación se abortaría. El usuario B, que recibe este mensaje, tras encontrar en esa lista un usuario autenticado en común genera un nuevo mensaje de tipo D2 incluyendo el hash de cada uno de los identificadores de los usuarios que haya autenticado hasta entonces, y un grafo aleatorio de n vértices creado a partir de la clave pública del usuario común. A recibe el mensaje D2 y genera un mensaje D3 que envía a B, conteniendo otro grafo aleatorio de n vértices creado a partir de la clave pública del usuario común.

Tras la fase de mensajes D se inicia el proceso de demostración mutua de conocimiento sobre la clave pública común, con los grafos intercambiados. La usuaria A crea un grafo isomorfo a partir de su grafo aleatorio y lo envía a B en un mensaje Z1, y B hace lo mismo. Obsérvese que la clave pública debe tener una longitud exacta de representación binaria de valor $\frac{n(n+1)}{2}$, ya que a partir de ella se debe generar un grafo cuya matriz de adyacencia de tamaño nxn tenga la particularidad de poseer dos 1's por fila y columna, puesto que la clave se corresponde con un circuito hamiltoniano en el grafo aleatorio. Por tanto, el procedimiento implica que se construye una matriz binaria, teniendo en cuenta que los elementos de la diagonal principal son ceros, y los elementos sobre ella se corresponden con los bits de la clave publica, que se repiten de forma especular bajo la diagonal, formando una matriz simétrica.

Ejemplo: La clave pública, que en base decimal es 12869, se corresponde con una representación binaria correcta ya que conduce a la matriz de adyacencia de un circuito hamiltoniano. Mediante la inyección aleatoria de '1's en la representación binaria de la clave pública, se logra generar un grafo en el que la clave pública es solución, y a partir de un vector aleatorio de permutación de filas se genera un grafo isomorfo a enviar en

el mensaje D5. Todos estos parámetros se muestran mediante un ejemplo a continuación.

Clave pública en base decimal: 12869
Clave pública en base binaria: 011001001000101 (Longitud de 15 bits)
Matriz correspondiente a la clave pública (Dos '1's por fila y columna):

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

A la clave pública en binario se le inyectan 5 '1's, aleatoriamente:
0 1 1 1 1 1 0 1 1 0 1 0 1 1 1
A partir de esta nueva ristra de bits, se construirá una matriz de adyacencia:

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Vector aleatorio de permutación de filas :

$$[6, 5, 3, 4, 2, 1]$$

Matriz de adyacencia del grafo isomorfo:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

La siguiente batería de mensajes son los retos y respuestas de una demostración de conocimiento nula, y comienzan con el envío por parte del usuario B, de una pregunta aleatoria binaria. Un cero significa: ¿Existe equivalencia entre el grafo aleatorio y el grafo isomorfo?. Un uno tiene asociada la pregunta: ¿Existe un circuito hamiltoniano en el grafo isomorfo?. Este mensaje Z2 le llega a la usuaria A, quien responde con un mensaje Z3, que contiene toda la información necesaria para que el usuario B pueda comprobar la pregunta que envió. De esta manera el usuario B puede fiarse un poquito más de la usuaria A si obtiene respuesta positiva con los datos obtenidos. En ese caso, el usuario B vuelve a crear un grafo isomorfo a partir del grafo aleatorio y enviarlo en un mensaje Z1. De nuevo B envía una pregunta Z2 y A responde con un mensaje de tipo Z3. Los mismos pasos en sentido inverso, de demostración de B hacia A, se realizan en paralelo. Si ambos usuarios confirman de nuevo la información recibida en esta segunda iteración, empieza la fase de intercambio de información de ambos usuarios.

En primer lugar el usuario B envía un mensaje E1 con el cifrado de su clave pública, usando como clave secreta la clave común a ambos, y en paralelo la usuaria A hace lo mismo. A continuación A envía al usuario B en un mensaje E2 el cifrado de una clave de sesión usando la clave pública del receptor, y B hace lo mismo. En un último mensaje E3 A envía a B el cifrado de su lista de claves públicas de otros usuarios autenticados, usando la clave de sesión recibida, y B hace lo mismo.

A partir de entonces ambos usuarios ya tienen todos los datos necesarios del otro usuario, y lo reconoce como autenticado.

Una de las medidas que se tomaron para medir la eficacia del algoritmo, fueron los tiempos que tardaban dos usuarios en autenticarse, en distintas situaciones, como podemos ver en la Tabla 2.

	Cobertura	**Simulador**	**Terminal Móvil**
Con 2 usuarios	Sin GPS	menor a 0.5	3 a 5
	Con GPS	menor a 1	5 a 7
Con 3 usuarios	Sin GPS	menor a 1	7 a 10
	Con GPS	menor a 2	12 a 15
Con más de 3 usuarios	Sin GPS	menor a 1.5	7 a 10
	Con GPS	menor a 2	12 a 20

Tabla 2. Tiempo (en segundos) de autenticación

II-D. Módulo de Detección de Eventos

El módulo de detección de eventos persigue el propósito práctico de las VANETs. Actualmente existen tres tipos de eventos de tráfico que VAiPho es capaz de detectar y transmitir.

II-D1. Eventos de atasco: Los eventos de atascos permiten informar a los usuarios de VAiPho sobre la existencia cercana de un atasco o congestión de tráfico, lo que les puede permitir optar por una ruta que lo evite. El principio básico que se esconde detrás de la detección de este evento es la comprobación de que el vehículo circula a una velocidad muy reducida respecto a la permitida en la vía en que se encuentra. Además, antes de retransmitir el correspondiente anuncio en modo broadcast, el evento de atasco es corroborado por otros vehículos cercanos mediante el módulo de agregación de datos, para así proporcionar la garantía de validez necesaria al anuncio del evento.

II-D2. Eventos de posibles aparcamientos libres: Este tipo de eventos permiten informar al usuario que maneja VAiPho, de posibles plazas de aparcamiento disponibles que estén cercanas al lugar donde el vehículo transita y con cobertura GPS. El algoritmo desarrollado se basa en que una plaza de aparcamiento se libera justo cuando el vehículo que la ocupaba arranca su vehículo, transmitiendo este hecho a los demás vehículos de la zona que anden buscando plazas de aparcamiento, para lo cual la interfaz de VAiPho proporciona la opción correspondiente. En todo caso se trata de una posible plaza de aparcamiento y no de una plaza segura de aparcamiento, ya que se pueden dar diversas circunstancias entre las cuales están que esa plaza la ocupe otro vehículo que llegue antes, o bien que se trate de una plaza de aparcamiento no pública, entre otros casos.

II-D3. Eventos de localización del vehículo: Por último, existe una utilidad de VAiPho que automáticamente almacena la posición GPS del vehículo al aparcarlo, de manera que permite al usuario recuperar la información sobre dónde lo dejó aparcado guiándole hasta su posición en modo peatonal, en caso de que se haya olvidado de la situación exacta del aparcamiento, situación que suele ser una circunstancia bastante común en grandes ciudades y aparcamientos al aire libre.

II-E. *Módulo de Agregación de Datos*

Tal como se ha mencionado, el módulo de agregación de datos tiene como finalidad la comprobación de coincidencias en la detección de atascos en tiempo real, para evitar mensajes malintencionados en la red, tratando de aportar garantías de veracidad de los eventos transmitidos. Cuando un usuario detecta un posible atasco, lo comunica a la red empezando un envío de mensajes que finalizan con la conclusión sobre la veracidad o no del evento en cuestión. Los usuarios que puedan corroborar el evento recibido, reenvían el mensaje del evento agregándole su firma digital para aportar garantía de veracidad. De esta manera los usuarios que reciban los mensajes del evento sólo lo tienen en cuenta y lo agregan a su base de datos de eventos, si dicho mensaje contiene un número mínimo de firmas válidas, que en la implementación prototipo actual está establecido en cinco. En ese momento el evento pasa de ser un posible atasco a ser considerado un atasco real.

II-F. *Módulo de Posicionamiento*

Uno de los aspectos más críticos de la implementación de VAiPho para Symbian fue lo concerniente a la tecnología de geoposicionamiento. Surgieron muchos problemas para poder mostrar gráficamente lo que VAiPho es capaz de detectar. La solución temporal escogida en la implementación actual en Symbian, ha consistido en representar los eventos sobre un fondo de color, proporcionando referencias al usuario sobre su posición con respecto a los eventos detectados. Mientras en otras plataformas no ha habido problemas con el uso de mapas, en el caso de Symbian la solución escogida es temporal hasta que se pueda sustituir ese fondo de color por un mapa, bien sea creando un módulo para gestionar el mapa propio, o utilizando librerías externas de desarrolladores especializados en navegación GPS.

II-G. *Módulo Bluetooth*

Una de las premisas de la aplicación VAiPho es la de servir como herramienta de ayuda al conductor. Para ello es necesario que su utilización no afecte en ningún momento la atención del conductor en la carretera. Por tanto, a la vez que los eventos se representan en el mapa, también se comunican mediante anuncios de voz. Además, tanto la iniciación como el apagado de la aplicación es totalmente automática. Para esta labor entra en juego la tecnología Bluetooth.

El concepto que se tuvo en cuenta para que VAiPho se inicie y apague automáticamente consiste en detectar que el vehículo arranque o se apague. Para conocer esta circunstancia se tiene en cuenta el dispositivo Manos Libres del vehículo, que se inicia o se apaga al mismo tiempo que lo hace el automóvil. De esta forma el móvil es capaz de detectar cuándo el Bluetooth del vehículo se inicia o se apaga, y en ese momento la aplicación hace lo mismo.

III. Interfaces de VAiPho

VAiPho se agrupa en una serie de interfaces que sirven en conjunto para funcionar como una sola aplicación distribuida.

III-A. *VAiPho WatchDog*

Esta interfaz es la encargada de iniciar y apagar automáticamente VAiPho. Para ello, como se ha explicado, se hace uso del Bluetooth, ya que se espera a que se genere el evento de sincronización del móvil con el vehículo a través del dispositivo Manos Libres para iniciar o apagar la interfaz VAiPho Automatic, que se explica más adelante. En la figura 2 se puede ver parte del aspecto visual de dicha interfaz para la plataforma Symbian.

Figura 2. Interfaz gráfica de VAiPho WatchDog

III-B. *VAiPho User Interface*

Esta interfaz permite la configuración de todos los parámetros variables de VAiPho. Como se puede ver en la figura 3, la interfaz VAiPho User posibilita el uso de la aplicación consistente en detectar dónde está el vehículo aparcado.

Figura 3. Interfaz gráfica de VAiPho User

III-C. *VAiPho Automatic*

Se puede considerar a esta interfaz como la principal. Está relacionada con múltiples aspectos importantes de VAiPho, como son la autenticación, detección y notificación de eventos al usuario, agregación de datos y comunicaciones. En la figura 4 se puede observar cómo vería el conductor el prototipo de VAiPho para Symbian.

Por último, destacar el consumo de batería que conlleva la utilización de las diferentes interfaces de VAiPho para Symbian. En la Tabla 3 se puede observar el tiempo útil de duración de la batería con las diferentes interfaces.

Interfaces	**Tiempo en horas**
Smartphone sin VAiPho	84
Smartphone con VAiPho WatchDog	30
Smartphone con VAiPho Automatic	4

Tabla 3. Tiempo útil de batería

Figura 4. Interfaz gráfica de VAiPho Automatic

IV. Conclusión

La siguiente generación de Internet, la Internet de las Cosas, está tocando las puertas del presente cada día con más fuerza. Tener a cualquier objeto localizado desde cualquier punto del planeta será posible en un futuro muy próximo. La posibilidad de que los objetos se fusionen con el entorno e interactuen entre sí es ya prácticamente un hecho. Uno de los tópicos con más futuro dentro de este paradigma es la gestión del tráfico mediantes el uso de VANETs, lo que implica la identificación de cada vehículo en tiempo real sin poner en peligro su privacidad. Sin embargo, la tecnología avanza a un ritmo desmesurado en comparación con el avance de la seguridad que debe incorporar. Además, implantar las VANETs de la forma en que se ha propuesto en la bibliografía provocaría un gasto bastante elevado tanto a las administraciones públicas que deberían instalar y mantener una infraestructura de comunicaciones en las carreteras, como a los usuarios que tendrían que adaptar o cambiar sus vehículos.

Gracias a la aplicación VAiPho propuesta, cuya implementación se ha descrito en este trabajo, se podrán evitar esas inversiones económicas, poniendo al alcance de cualquier conductor el uso de la red vehicular actualmente. Basándose en ese mundo de objetos inteligentes interconectados del que versa la Internet de las Cosas, un simple teléfono móvil servirá para que cualquier vehículo acceda a esta red y pueda así conocer todo lo acaecido en las carreteras en tiempo real. Las comunicaciones en VAiPho han sido implementadas de forma totalmente segura gracias a los algoritmos criptográficos que incluye, por lo que se da solución a esa seguridad extra que tanto se añora en la evolución exponencial de las tecnologías. Además la detección automática de eventos proporciona plena confianza sobre su veracidad ya que permite la detección de mensajes falsos erróneos o malintencionados.

En particular, aquí se ha descrito la primera versión concerniente a la plataforma Symbian de los teléfonos Nokia, permitiendo la compatibilidad con otras plataformas como Maemo y Meego. En cuanto a trabajos futuros concretos destacamos la conveniente mejora en la interfaz VAiPho WatchDog para reducir el consumo de batería. Actualmente VAiPho permite detectar congestiones y atascos, posibles plazas de aparcamiento libres, situación exacta donde se ha dejado aparcado el vehículo, además de ofrecer una plataforma de publicidad geolocalizada. Sin embargo, en el futuro el abanico de posibles nuevas aplicaciones es realmente espectacular. Imaginar que un conductor con su teléfono móvil sea capaz de ayudar a la gestión de ese tráfico de manera transparente para él, o que VAiPho sea capaz de subir a la nube la información de los atascos en tiempo real o las necesidades de aparcamientos libres de cualquier zona del mundo, es realmente una posibilidad cercana. Poder orientarse en zonas sin cobertura GPS como aparcamientos de centros comerciales, pueden dar cabida a futuras aplicaciones que implemente nuestro sistema VAiPho, entre otras muchas. El límite, en este caso, lo pone la imaginación.

Referencias

[1] Anton E. y Duarte O. 2002. Group key establishment in wireless ad hoc networks. Workshop on Quality of Service and Mobility 2002.

[2] Armknecht F., Festag A., Westhoff D. y Zeng, K. 2007. Cross-layer privacy enhancement and non-repudiation in vehicular communication. 4th Workshop on Mobile Ad-Hoc Networks (WMAN).

[3] Blom R. 1985. An Optimal Class of Symetric Key Generation Systems. Advances in Cryptology. LNCS, vol. 209, páginas 335−338.

[4] Caballero-Gil C. (2011). Soluciones para la Autenticación y Gestión de Subredes en MANETs y VANETs. Tesis Doctoral. Universidad de La Laguna. Dir.: Pino Caballero Gil.

[5] Caballero-Gil P., Caballero-Gil C. y Molina-Gil J. 2010. Sistema de comunicaciones seguras en una red ad-hoc vehicular espontánea y autogestionada. Patente Nº: P201000865. Universidad de La Laguna. Tenerife. Spain

[6] First ACM Workshop on Vehicular Ad Hoc Networks, 2004 (VANET 2004). Loews Philadelphia Hotel, Philadelphia, PA, USA.

[7] Hubaux J.P., Capkun S. y Luo J. 2004. The Security and Privacy of Smart Vehicles.

[8] Martín-Fernández F. (2011). Implementación de comunicaciones seguras en la plataforma Symbian para asistencia a la conducción. Proyecto fin de Carrera. Universidad de La Laguna. Dir.: P. Caballero-Gil y C. Caballero Gil.

[9] Molina-Gil J. (2011). Nuevas Herramientas de Seguridad Cooperativa para Redes Ad-Hoc Vehiculares. Tesis Doctoral. Universidad de La Laguna. Dir.: Pino Caballero Gil.

[10] Nikodem J. y Nikodem M. 2007. Secure and Scalable Communication in Vehicle Ad Hoc Networks. Eurocast 2007, páginas 1167−1174.

[11] Parno B., Perrig A. 2005. Challenges in securing vehicular networks. Proceedings of the ACM Workshop on Hot Topics in Networks.

[12] Perrig A., Canetti R., Tygar J.D. y Song D. 2002. The TESLA Broadcast Authentication Protocol. RSA CryptoBytes 5, páginas 2-13.

[13] Raya M. y Hubaux, J.P. 2005. The security of vehicular ad hoc networks. 3rd ACM Workshop on Security of Ad hoc and Sensor Networks-SASN 2005, páginas 11−21.

[14] Raya M. y Hubaux, J.P. 2007. Securing vehicular ad hoc networks. Journal of Computer Security (special issue on Security of Ad Hoc and Sensor Networks) 15(1), páginas 39−68.

[15] Raya M., Papadimitratos P., Aad I., Jungels D. y Hubaux, J.P. 2007. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications 25(8), páginas 1557−1568.

[16] Raya M., Papadimitratos P. y Hubaux, J.P. 2006. Securing vehicular communications. IEEE Wireless Communications Magazine 13(5), páginas 8−15.

[17] Steiner M., Tsudik G. y Waidner M. 1996. Diffie-Hellman Key Distribution Extended to Group Communication. ACM Conference on Computer and Communications Security, páginas 31−37.

[18] Tsang P. y Smith S. 2008. PPAA: Peer-to-Peer Anonymous Authentication, ACNS 2008, páginas 55−74.

[19] Zarki M.E., Mehrotra S., Tsudik G. y Venkatasubramanian N. 2002. Security issues in a future vehicular network. Proceedings of European Wireless 2002.