XIV Jornadas de Ingeniería Telemática.
JITEL 2019.
Universidad de Zaragoza.

Actas de las XIV Jornadas de Ingeniería Telemática (JITEL 2019), Zaragoza (España), 22-24 de octubre de 2019.

ISBN: X-XXXX-XX-XXX-X
DOI: XXXXXX

Desarrollo de un semáforo inteligente basado en comunicaciones seguras

Manuel Montenegro-Gómez, Isaac Agudo
Departamento de Lenguajes y Ciencias de la Computación,
Universidad de Málaga
{mmg,isaac}@lcc.uma.es

***Resumen*—En los nuevos paradigmas de movilidad surgidos durante los últimos años y en aquellos aún por llegar ha quedado patente la necesidad de modernizar la infraestructura viaria y los elementos de señalización y gestión del tráfico. En el presente trabajo se presenta una propuesta para esta nueva generación de dispositivos de gestión del tráfico: un prototipo de semáforo inteligente conectado que implementa diversas medidas de seguridad. Además de las tradicionales señales luminosas, los usuarios de la vía pueden conocer a través de sus dispositivos el estado del semáforo, además de otra información complementaria a través de la difusión de mensajes BLE firmados con criptografía de curva elíptica. A su vez, el semáforo puede ser gestionado remotamente a través de la tecnología LTE Cat M1 protegida por TLS. Esto abre la puerta, entre otros, a facilitar el tránsito de los vehículos de emergencia cuando estos se acercan a un cruce o modificar el tiempo de los estados del ciclo en función de las necesidades del tráfico.**

***Palabras Clave*—semáforo inteligente, sistemas de transporte inteligente, seguridad en las comunicaciones, bluetooth low energy, curva elíptica, nrf52840, tls.**

I. INTRODUCCIÓN

Todo parece indicar que, en los próximos años, el sector de la automoción será el epicentro de profundas transformaciones tecnológicas. La aparición de nuevos paradigmas de movilidad, una flota de vehículos creciente en número, la implantación de restricciones anticontaminación, la modernización de los vehículos, cada vez con mayor capacidad de asistencia al conductor e incluso de tomar el control, así como el uso de nuevos medios de transporte multimodales compartidos y los vehículos de movilidad personal (VMP) son algunos de las piezas del puzzle que conforman y motivan la investigación y desarrollo de los Sistemas de Transporte Inteligente.

Los medios tradicionales de gestión del tráfico, tales como semáforos y señales viales, tienen ahora la necesidad de aportar una mayor cantidad de información, dotándola de una mayor seguridad, rapidez y tolerancia a fallos, en la medida en que esta información se hace crítica para el funcionamiento de estos nuevos sistemas.

Como ejemplo, la compañía Audi lleva más de dos años prestando un servicio de información de semáforos Audi Traffic Light Information [1] con las funciones Time-to-Green en EEUU, y este año 2019 comienzan las pruebas en Europa. También se ha añadido la funcionalidad Green Light Optimized Speed Advisory (GLOSA), servicio que se apoya en una infraestructura paralela a los semáforos ya existentes y que aporta información de los semáforos cercanos basándose en su posición GPS.

Una alternativa a la propuesta por Audi sería proporcionar a los semáforos y demás señales de tráfico un mecanismo de comunicación directo con los vehículos. En este sentido, el desarrollo de un semáforo inteligente seguro trata de incorporar una solución confiable y económica a este ecosistema, que englobe no solo a los vehículos tradicionales sino a también los VMP.

En el presente trabajo se ha implementado un mecanismo seguro de intercambio de información viaria basado en el protocolo Bluetooth Low Energy versión 5.0, disponible en la mayoría de los teléfonos inteligentes [2], de forma que los usuarios pueda interactuar con las señales inteligentes usando su teléfono. Esto requiere del desarrollo de una infraestructura de clave pública que permita autenticar a los dispositivos desplegados en las vías, siguiendo para ello el mismo camino que los estándares ITS [3] (Intelligent Transport Systems).

Otro requisito central es permitir que determinadas señales viarias puedan estar conectadas a internet. Para ello, se ha analizado el uso del protocolo TLS sobre tecnologías estándar de la 3GPP para Low Power Wide Access Networks (LPWAN). [4]

Para el desarrollo del prototipo se ha utilizado un microcontrolador (nRF52840[1]) de Nordic Semiconductor, con soporte para la version 5.0 de Bluetooth Low Energy y que además cuenta con capacidad de realizar cálculos criptográficos acelerados por hardware.

[1]https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52840

II. SEGURIDAD EN ITS

El ETSI (European Telecommunications Standards Institute) ha elaborado un marco de estandarización sobre las comunicaciones en los ITS que engloba todo tipo de comunicaciones entre los vehículos y su entorno, así como aspectos relativos a la seguridad y a la privacidad. (informe técnico ETSI TR 101 607 [3]). La ETSI también define un conjunto de aplicaciones para la mejora del tráfico basadas en las comunicaciones dedicadas de corto alcance (DSRC por sus siglas en inglés) o los ITS cooperativos (c-ITS).

Además, el Institute of Electrical and Electronics Engineers (IEEE) define el estándar IEEE 802.11p [5] para el acceso inalámbrico en entornos vehiculares (WAVE, por sus siglas en inglés).

Los mensajes de tipo Cooperative Awareness Message (CAM), definidos en la norma europea ETSI EN 302 637-2 [6], están diseñados para ser transmitidos de punto a multipunto y transportan información sobre el vehículo o el entorno. Van además firmados digitalmente, como figura en el estándar [7] e incluyen la información siguiente:

- Versión del protocolo.
- Cabecera: información del dispositivo que generó la firma, hash del certificado asociado al dispositivo, marca de tiempo de generación del mensaje e identificación de la aplicación.
- Payload o carga útil del mensaje.
- Firma digital del mensaje mediante el algoritmo ECDSA con la curva NIST P-256.

Para distribuir las claves públicas necesarias para verificar los mensajes CAM, se define también un formato compacto de certificado digital, con un tamaño de 132 octetos con los campos siguientes:

- Versión del certificado.
- Identificador del dispositivo firmante del certificado.
- Información sobre a quién va dirigido el certificado.
- Clave pública de la firma.
- Firma digital, codificada como un par de puntos.

En el cuadro I se reflejan los tamaños de cada unos de los campos de los mensajes mencionados.

Cuadro I: Formato del mensaje CAM

Certificado CAM		Mensaje seguro CAM	
Elemento	Octetos	Elemento	Octetos
version	1	version	1
signer	9	header	24
subject	2	payload	x
public key	44	signature	68
validity	10		
signature	66		

III. ARQUITECTURA DEL SISTEMA

La arquitectura consta de dos planos: el de gestión y el de difusión, tal como se ilustra en la Figura 1.

Plano de difusión

El plano de difusión contiene dos actores. De un lado, se encuentra el dispositivo en modo baliza. Mediante mensajes de difusión BLE se encuentra difundiendo a tiempo real el estado actual del semáforo. Esto incluye

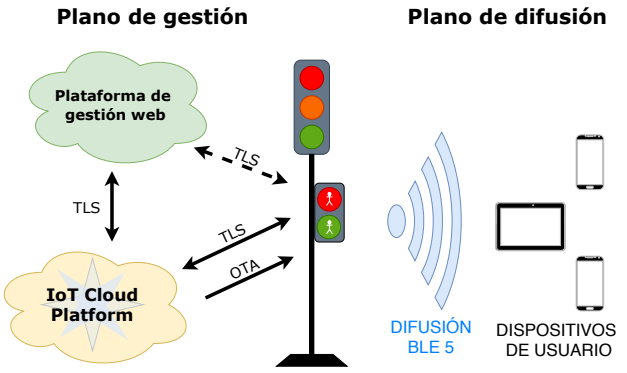

Figura 1: Arquitectura del sistema diseñado

información como el estado actual en el que se encuentra, el tiempo restante para el siguiente cambio de estado o su posición GPS a fin de poder ser ubicado.

Estas tramas son firmadas antes de ser emitidas e incluyen información adicional como longitud de la trama o una marca temporal a fin de asegurar su legitimidad y validez. Por tanto, es el semáforo el encargado de generar la firma.

En el lado de los dispositivos de usuario, estas tramas son recibidas y corresponde al mismo verificar que la firma es correcta. Esto se realiza haciendo uso del certificado que es transmitido en la trama y que corresponde de manera unívoca a cada dispositivo.

Si bien los *certificados* de los dispositivos se envían junto con la trama de difusión, esto limita el tamaño disponible para la carga útil de la trama. Actualmente se están analizando estrategias de distribución más eficientes.

Plano de gestión

Por otro lado, el plano de gestión es el encargado de dotar de lógica al dispositivo. En primer lugar tenemos una plataforma web, encargada de gestionar cada dispositivo de la infraestructura. La plataforma de gestión contiene una base de datos con la ubicación y estado a tiempo real de cada uno de los dispositivos.

La gestión incluye cambios en los tiempos destinados a cada estado del semáforo en función de las características actuales del tráfico, apertura o cierre de semáforos según convenga al paso de un vehículo de emergencia, desactivación o activación de semáforos, etc.

La plataforma web podría comunicarse directamente con los dispositivos de la carretera, pero la tendencia actual sería usar una plataforma IoT intermedia que haga de pasarela entre los semáforos y la plataforma de gestión. Resulta conveniente la utilización de algún estándar de gestión IoT tal como MQTT o CoAP, aunque en nuestro caso particular hemos usado la plataforma de gestión IoT de la empresa *Particle*, que gestiona los dispositivos desplegados y permite aplicar actualizaciones del firmware de los dispositivo si fuera necesario con un mínimo esfuerzo en el desarrollo.

IV. Comunicaciones infraestructura a vehículo

Para el desarrollo de este prototipo se ha optado por BLE frente a las tecnologías tradicionales para c-ITS debido su menor coste y disponibilidad inmediata en un mayor número de dispositivos personales. Dado que por requisitos de diseño la comunicación debe realizarse de punto a multipunto, se ha considerado el uso de mensajes BLE de difusión.

Los mensajes de difusión BLE, *Advertisement*, aparecen en la configuración Bluetooth Low Energy que fue introducida en la versión 4.0 del estándar Bluetooth. Supone una mejora frente a versiones anteriores del protocolo Bluetooth, en las cuales era necesario establecer una conexión punto a punto, para lo cual debía producirse una fase previa de descubrimiento y negociación.

Con la introducción de Bluetooth Low Energy se añadió esta capacidad de transmitir información de difusión, eliminando la necesidad de establecer una conexión previa entre dos dispositivos. Estos paquetes se transmiten en abierto y pueden contener cualquier tipo de información: desde instrucciones para realizar el emparejamiento entre dos dispositivos, hasta información sobre el entorno capturada por los sensores de un dispositivo. La información transmitida puede ser leída por cualquier dispositivo BLE situado en las cercanías y que esté funcionando en modo escáner.

La versión 5.0 del estándar Bluetooth introdujo algunas nuevas características a BLE [8]: mayor tasa de transferencia, alcance más amplio, mayor capacidad de transmisión en difusión e incremento de la coexistencia entre canales de frecuencia. De estas nuevas características, resultan de especial interés para el dispositivo desarrollado las siguientes:

- Alcance amplio o *Long Range*. Para conseguir un mayor alcance de la aplicación sin comprometer el consumo energético, se ha introducido codificación de tipo Forward Error Correction (FEC) en la capa física del estándar Bluetooth. Al utilizar esta característica, la información es codificada antes de ser enviada. Esto se traduce en una mayor sensibilidad a cambio de una tasa de transmisión menor.
- Mensajes de difusión extendidos o *Extended Advertising*. En esta versión de la especificación Bluetooth se ha rediseñado la capa de transporte. Existen tres canales para los mensajes de difusión (canales 37, 38 y 39) que tienen una capacidad máxima de 31 bytes. En esta nueva versión, cuando el mensaje ocupa más de 31 bytes, hasta un límite de 255 bytes, se negocia un canal de datos para transmitir el mensaje, y los datos son transmitidos en el canal elegido.

Si bien no todos los dispositivos móviles inteligentes tienen soporte actualmente para BLE versión 5.0 con estas dos extensiones (se ha confirmado el soporte en Google Pixel 3, Samsung S10+ y OnePlus 6), cabe esperar que el número de móviles con soporte para estas dos extensiones aumente conforme salgan al mercado nuevos terminales.

En el ámbito del presente trabajo solo se considera la emisión de información desde la infraestructura hacia los usuarios. Más concretamente, únicamente se trata la comunicación desde el semáforo inteligente a los usuarios de la vía. En este supuesto, la información facilitada es pública, por lo que no se considera determinante la protección de la privacidad ni la confidencialidad en el canal de difusión.

La solución que se propone consta de una sola trama en la que se incluye tanto la carga útil, como la firma de los datos y un certificado compacto del dispositivo. La estructura de los mensajes se encuentra representada en la Figura 2.

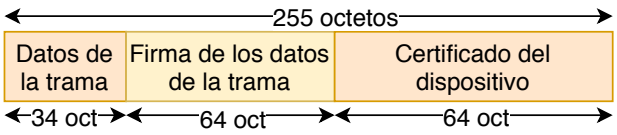

Figura 2: Estructura de mensaje advertising BLE 5

Como se puede ver, la trama consta de tres campos principalmente:

- Datos de la trama: donde se encuentran los datos a transmitir. Aquí se encuentra codificado en hexadecimal los siguientes campos: el identificador del tipo de dipositivo (1 oct.), las coordenadas GPS (8 oct.), la dirección hacia la que el semáforo está apuntando (4 oct.), el rumbo hacia el que la señal lumínica del semáforo afecta (vehículos que van a seguir rectos, vehículos que van a girar a derecha o izquierda, etc. 4 oct.), el estado actual (1 oct.) y el tiempo restante en segundos del estado actual (1 oct.).
- Firma de los datos de la trama: se trata de una firma del campo anterior mediante el algoritmo ECDSA. Se emplea curva elíptica de tipo Secp256k1.
- Certificado del dispositivo: se trata de un certificado digital reducido único para cada dispositivo generado por la CA de la plataforma.

La estructura del certificado reducido diseñado en este trabajo se puede encontrar en la Figura 3.

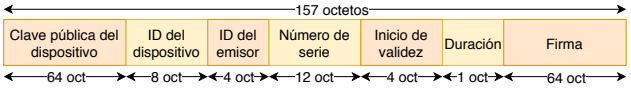

Figura 3: Trama del certificado reducido

Este formato de certificado, al igual que el propuesto en c-ITS, es una alternativa más compacta al estándar X.509 de UIT [10]. Aún así, en nuestro caso este mensaje ocupa 157 octetos frente a los 132 octetos del certificado de los mensajes CAM. Esta diferencia se debe principalmente al tipo de representación elegida para la clave pública, que es representada de forma comprimida (únicamente un punto de la curva y el signo del otro punto) usando 33 octetos en lugar de 64 octetos. En nuestro caso, la SDK criptográfica del nRF52840 utiliza una representación mediante dos puntos, es decir, se necesitan 64 octetos para almacenar

la clave pública. Como puede verse en la Figura 3, el certificado consta de 7 campos:

- Clave pública del dispositivo: Se trata de la clave pública generada por el dispositivo.
- ID del dispositivo: Es un identificador único del dispositivo que está emitiendo los mensajes de difusión. Es asignado por la plataforma de gestión de la infraestructura. En nuestro caso, se ha optado por que el identificador corresponda a las coordenadas GPS del dispositivo, pues no pueden coincidir dos dispositivos en las mismas coordenadas exactas. Las coordenadas GPS se codifican usualmente en 4 bytes.
- ID del emisor: Se trata de un identificador único de la CA que emite el certificado.
- Número de serie: Identifica al certificado en si. Es asignado por la CA.
- Inicio de validez: Es la marca temporal del momento a partir del cual el certificado es válido.
- Duración: Tiempo, medido en días, durante el cual es certificado es válido.
- Firma del certificado reducido: Es la firma digital de todos los campos anteriores.

V. Gestión remota del dispositivo usando LPWAN

LTE Cat M1 es una tecnología de telecomunicación LPWAN (Low Power Wide Area Network) cuyo estándar ha sido desarrollado por el 3GPP (3rd Generation Partnership Project). La especificación para esta tecnología se incluye en el 3GPP Release 13 [4], e incluye las tecnologías LPWAN LTE Cat NB1 y Narrow Band IoT.

Aunque ambas son tecnologías de bajo consumo, orientadas al IoT (Internet of Things), existen diferencias entre ambas [9]. Dada la volatilidad de los datos transmitidos en los ITS, una de las características más valoradas es el menor retardo posible. Es por esto que se ha decidido usar la tecnología LTE Cat M1, con una latencia de 50 a 100ms, frente a NB-IoT, cuya latencia es de varios segundos.

Particle provee servicios de gestión de los dispositivos IoT que fabrica a través de su nube de gestión, simplificando la tarea de gestionar un gran número de dispositivos y sus respectivas comunicaciones.

En nuestro prototipo[2] se usa Particle Cloud [11] como puente entre la plataforma de gestión web y los dispositivos desplegados. La nube de Particle ofrece una API y una conexión segura mediante TLS, para que la plataforma de gestión web acceda a la información de los sensores. Por otro lado, la comunicación entre la infraestructura y los dispositivos se realiza de igual manera mediante TLS.

El esquema de las conexiones entre los elementos hardware del prototipo se encuentra en la Figura 4.

VI. Conclusiones y trabajo futuro

Se puede afirmar que se han cumplido todos los objetivos iniciales del trabajo: el tamaño de trama de los mensajes de difusión BLE extendidos nos permite incluir

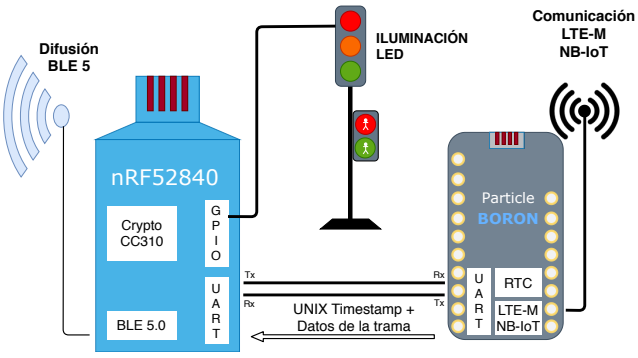

Figura 4: Esquema de conexiones elementos hardware del semáforo

en ellos la misma información que en el estándar c-ITS, con un nivel de seguridad equivalente. Además, las pruebas de campo nos permiten asegurar que la sobrecarga del sistema, gracias al uso del acelerador hardware criptográfico, es mínima.

Con respecto a la solución propuesta por Audi, el presente trabajo aporta una solución en la que las comunicaciones son realizadas directamente V2X (Vehicle-to-everything), sin la necesidad de una infraestructura de comunicación entre ambos.

La posibilidad de gestión remota segura del semáforo abre las puertas a nuevas aplicaciones que no requieran de un despliegue de fibra dedicado para la interconexión de estos con los centros de control.

Queda pendiente el diseño de un mecanismo para la distribución eficiente de los certificados de dispositivos. Algunas posibilidades que se barajan son:

- Puntos de distribución en las vías: A lo largo del territorio se sitúan balizas encargadas de difundir los certificados de los dispositivos de la zona.
- Distribuidos por el mismo dispositivo: El dispositivo se encarga de transmitir mensajes de difusión con los certificados, intercalados con los mensajes con información del estado.

Referencias

[1] El servicio de información de semáforos Audi Traffic Light Information llega a Europa. Fuente: http://prensa.audi.es/ 30/05/2019.
[2] Android Bluetooth Conectivity. Android Open Source Project. https://source.android.com/devices/bluetooth.
[3] ETSI TR 101 607 Technical Report. ETSI.
[4] Release 13 of 3GPP standard. https://www.3gpp.org/release-13.
[5] "IEEE Std. 802.11p-2010, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11, 2010.
[6] ETSI EN 302 637-2 European Standard. ETSI.
[7] ETSI TS 103 097 V1.2.1 Technical Specification. ETSI.
[8] Bluetooth 5 CS - Core Specification. Bluetooth SIG. 12/2016
[9] Differences between NB-IoT and LTE-M. Accent Systems. https://accent-systems.com/blog/differences-nb-iot-lte-m/.
[10] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF.
[11] Particle Device Cloud API. Particle Docs. https://docs.particle.io/reference/device-cloud/api/

[2]https://github.com/nicslabdev/MOTAM-nRF52_Beacons