Seguridad y Privacidad en un Sistema de Control de Acceso Distribuido para Zonas de Bajas Emisiones

XVII Reunión Española sobre Criptología y Seguridad de la Información

Santander – Octubre 2021

Dr. Carles Anglés Tafalla
Dr. Jordi Castellà Roca
Dr. Alexandre Viejo

Universitat Rovira i Virgili
Grup CRISES

UNIVERSITAT ROVIRA i VIRGILI

Introducción

Disminuir la **contaminación atmosférica** y conseguir una **mayor sostenibilidad** en la movilidad urbana es uno de los retos de las grandes ciudades.

- Uso racional de vehículos.
- Alta ocupación de vehículos.
- Vehículos eléctricos.

Madrid – nube de contaminación

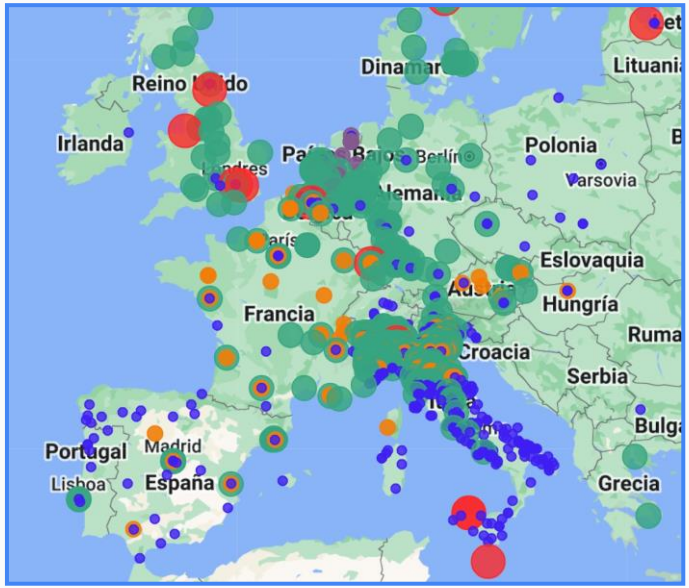
Barcelona – nube de contaminación

Low Emission Zone (LEZ)

Zonas delimitadas donde se aplican **restricciones** o **penalizaciones** a los vehículos contaminantes.

Fomentar el uso de vehículos poco contaminantes:

- Vehículos híbridos.
- Vehículos sin emisiones.
- Vehículos eléctricos.



Ejemplo de LEZs

London

Barcelona

Stockholm

Problemas:

- *Son sistemas invasivos debido al uso indiscriminado de cámaras.*
- *Se requieren numerosas y/o grandes infraestructuras.*

Related work

En los últimos años, han aparecido propuestas **más respetuosas** con la **privacidad** de los usuarios [1, 2, 3, 4, 5] . Evitan el uso indiscriminado de cámaras para identificar los vehículos que circulan por la LEZ.

- Autenticación con la infraestructura (entrada/salida) mediante comunicación inalámbrica.
- La privacidad de los usuarios honestos se preserva durante el proceso.
- La infraestructura solo toma fotos si la validación falla o se omite.
- Una entidad centralizada, proveedor de servicios (SP), recopila las pruebas de acceso registradas, las verifica y las tarifica.

Problemática

Dependencia hacia **entidades centralizadas** para la validación de evidencias de accesos, calculo de sus tarifas y cobro de sus correspondientes cantidades.

Requiere la implementación, despliegue i mantenimiento de numerosas i/o costosas **infraestructuras**.

Contribuciones

Propuesta de un sistema distribuido y autónomo para gestionar los accesos a LEZs:

- Preserva la privacidad de los conductores honestos y puede identificar a los usuarios fraudulentos.
- No requiere infraestructuras de control de acceso. Hace uso de los sistemas de detección y comunicación avanzados de los vehículos.
- Elimina la presencia de entidades centralizadas en la verificación, tarificación y cobro de los accesos vehiculares a la LEZ.

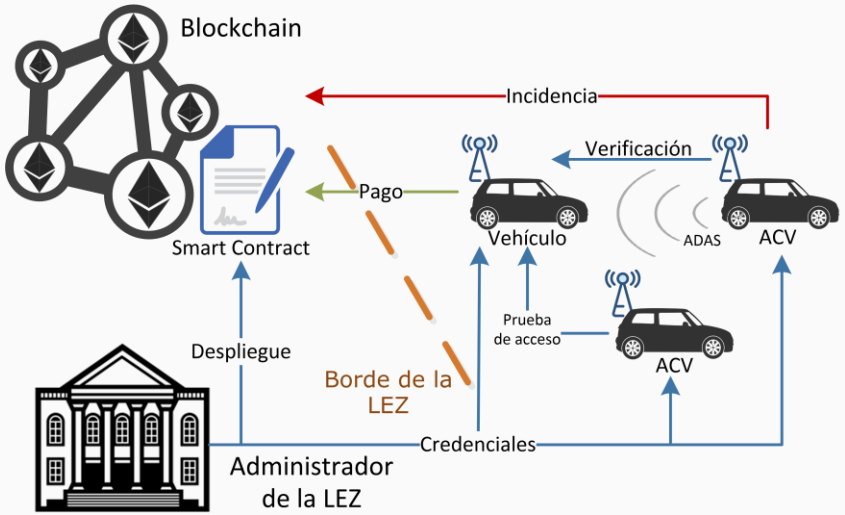
Modelo del sistema

Actores:

- Administrador de la LEZ (LA)
- Conductor (D) / Vehículo control de Acceso (ACV)
- Smart Contract de la LEZ (SC)

Fases:

- Configuración OBU
- Adquisición de Tokens
- Generación prueba de acceso / Control de acceso
- Pago / Verificación de Pago
- Anti-Fraude
- Renovación de alias temporal



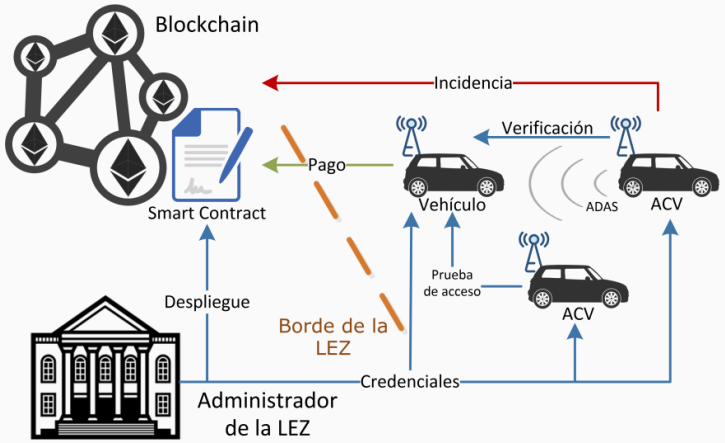
Fases del protocolo

1. Configuración de la OBU

- LA registra un vehículo a un conductor autorizado D.
- Se generan las credenciales para D, un alias temporal pareja de **claves asimétricas** (sk_D, pk_D) y **certificado** cert(pk_D).
- D genera una o varias **carteras digitales** $W(Sk, Pk)_1..W(Sk, Pk)_n$ con especificaciones Ethereum para interactuar con el SC.

2. Adquisición de divisa virtual

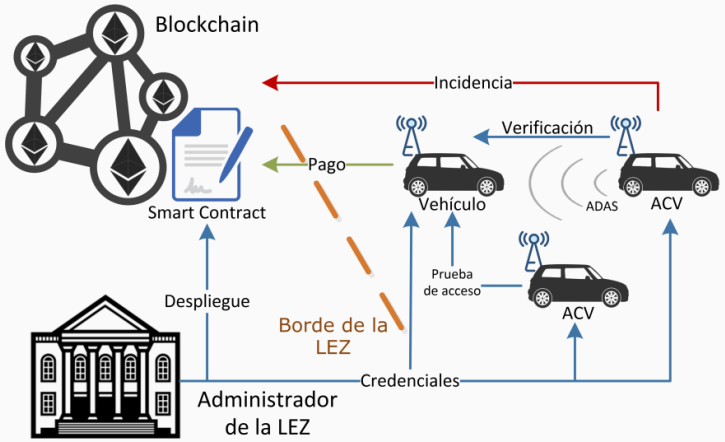
- D crea un cartera temporal W^T y adquiere monedas digitales para ella (p.e. portal online).
- Un mixer de criptomonedas que tranfiere los fondos de W^T *a* W.
- Evita que el vendedor vincule W con los datos bancarios de D.



Fases del protocolo

3. Generación prueba de acceso / Control de acceso

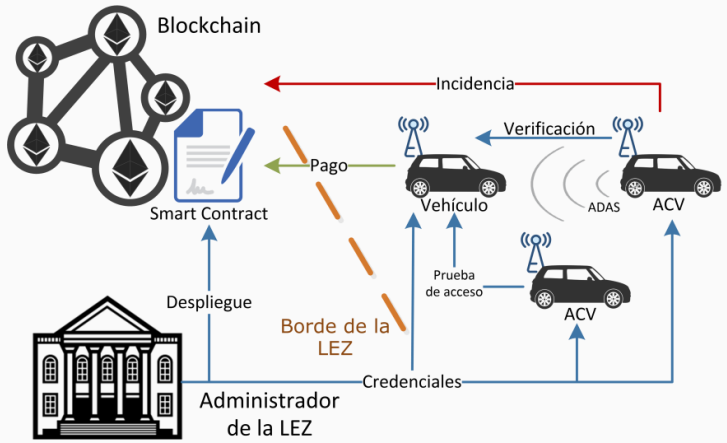
- Cuando los **sensores** delanteros/traseros del ACV **detectan** un D se inicia la generación/verificación de una prueba de acceso.
- Si **D no tiene prueba** de acceso, D y ACV validan **parámetros** (δ, $zona_{id}$, t_a, cat) de **estancia** en la LEZ. Ambos obtienen estas **pruebas firmadas** digitalmente por la parte contraria.
- D también recibe estos datos **firmados** por la **cartera digital del ACV**, permite su verificación on-chain por el SC (fase de pago).
- Si **D ya dispone** de una prueba de acceso**, D remite** su **prueba** (+timestamp) firmada. ACV la verifica y la **almacena**.



Fases del protocolo

4. Anti-fraude

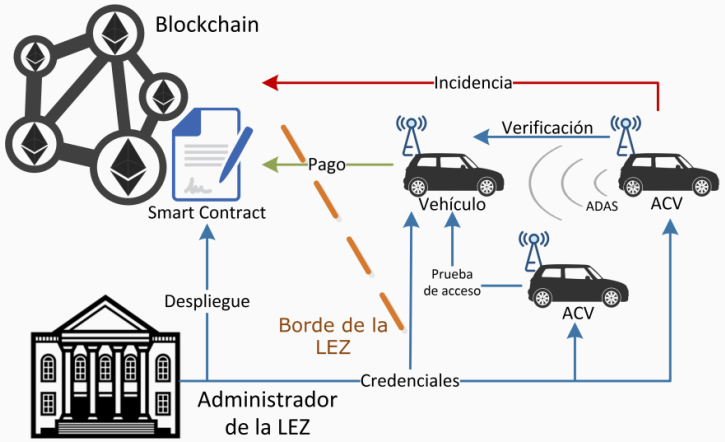
- Si D no responde o altera el protocolo anterior en algún paso, ACV sus cámaras delantera o trasera para **fotografiar** a D.
- ACV usa un sistema indicador de intensidad de la señal recibida (e.g. **RSSI** [6]) y las **localizaciones** recibidas para verificar que se trata del vehículo que detectan sus sensores. Propuesto en [4].
- ACV envía la foto, timestamp y geolocalización, firmada digitalmente a LA.
- Si LA acumula cierta cantidad de pruebas de distintos ACV, sanciona a D.
- LA remunera a los ACVs implicados.



Fases del protocolo

5. Pago

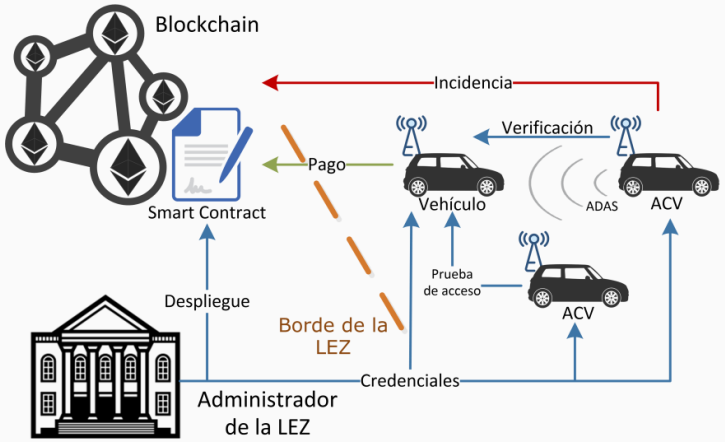
- D invoca el método “register access” del SC, con la **prueba de acceso** y **la firma digital** de la cartera de **ACV**.
- SC **verifica** la **firma digital** y **tarifica** en función de los datos (fecha, hora, cat., etc.) y las tarifas LEZ en el Blockchain.
- SC **transfiere** las criptomonedas correspondientes desde la cartera de D a las carteras de LA y ACV.



Fases del protocolo

6. Verificación del pago

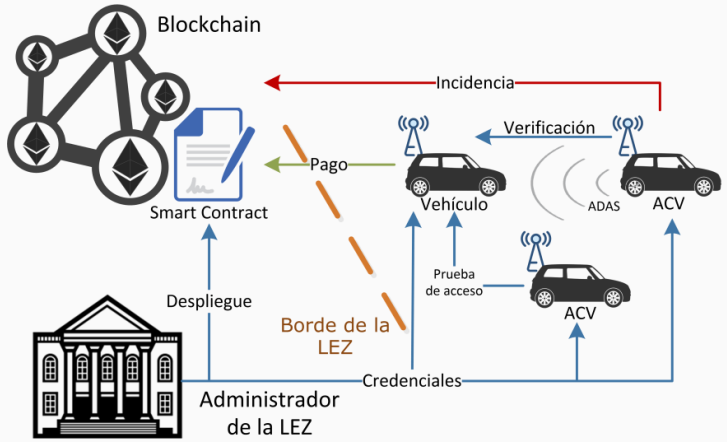
- Después de un tiempo los **ACVs con copia de la prueba** de acceso **verifican** el estado del acceso δ.
- Si el acceso **no** está **publicado** en el blockchain o su estado figura como **no pagado**, el ACV publica una **incidencia** en el blockchain.
- El SC **verifica** que se cumplen las condiciones necesarias para que ACV abra una incidencia.
- Con la incidencia, ACV publica en el Blockchain su copia de la prueba de acceso, firmada por D.



Fases del protocolo

7. Renovación del alias temporal

- Un usuario D puede renovar su alias temporal.
- Evita que se puedan vincular sus accesos a la LEZ.
- Implica regenerar sus claves y certificado digital
- En el proceso también se debería renovar la cartera digital.
- Las divisas virtuales entre carteras propias deben transferirse con un «mixer de criptomonedas» (no-enlazabilidad)



Conclusiones

Control de acceso totalmente distribuido para escenarios LEZ que preserva privacidad de los usuarios honestos.

- Nuestro sistema adopta la tecnología de los Smart contracts, y el subyacente Blockchain, para descentralizar la tarificación y cobro de los accesos a la LEZ
- Hace uso de los sistemas ADAS avanzados integrados en los vehículos de nueva generación para evitar el despliegue de infraestructuras.

Future work

- Implementación del sistema propuesto para verificar su viabilidad en un entorno relevante.
- Estudios basados en simulaciones para determinar el umbral/proporción de ACVs honestos sobre el total para garantizar la detección de fraude.

Proyecto FEM-IoT

Unió Europea
Fons europeu
de desenvolupament regional

Proyecto FEM-IoT: cofinanciado por el Fondo Europeo de Desarrollo Regional de la Unión Europea en el marco del Programa Operativo FEDER de Catalunya 2014-2020 con una ayuda del 50% del coste total.

https://femiot.cat/

References

[1] R. Jard -Cedó, M. Mut-Puigserver, M. M. Payeras, J. Castella-Roca, and A. Viejo, "Time-based low emission zones preserving drivers' privacy", Future Generation Computer Systems, vol. 80, pp. 558{571, 2018.

[2] R. Jard -Cedó, J. Castellà, and A. Viejo, "Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing", Security and Communication Networks, vol. 9, pp. 3197-3218, 2016.

[3] C. Anglès-Tafalla, J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capellà, and A. Viejo, , "Secure and privacy-preserving lightweight access control system for low emission zones," Computer Networks, vol. 145, pp. 13–26, 2018.

[4] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities", IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1592{1603, 2018.

[5] M. Hoffmann, V. Fetzer, M. Nagel, A. Rupp, and R. Schwerdt, "P4TC- provably-secure yet practical privacy-preserving toll collection, "Proceedings on Privacy Enhancing Technologies, vol. 3, pp. 62–152, 2020.

[6] R. S. Yokoyama, B. Y. Kimura, L. A. Villas, and E. D. Moreira,, "Measuring distances with rssi from vehicular short-range communications," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. IEEE, 2015, pp. 100–107.

Thanks!

Contact us:

carles.angles@urv.cat

jordi.castella@urv.cat

alexandre.viejo@urv.cat