Pruebas Basadas en el Entorno para la Detección de Ataques de Relay en Accesos a Zonas Restringidas

Carles Anglès-Tafalla*, Jordi Castellà-Roca*, Alexandre Viejo*,
M. Magdalena Payeras Capellà†, Macià Mut Puigserver†
*Departament d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili,
Av. Països Catalans 26, E-43007 Tarragona, Spain
{carles.angles,jordi.castella,alexandre.viejo}@urv.cat
†Departament de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears,
Ctra. de Valldemossa, km 7,5. E-07122 Palma, Spain
{mpayeras,macia.mut}@uib.es

***Resumen*—Las zonas de bajas emisiones (LEZ) son áreas urbanas donde el acceso de vehículos contaminantes está restringido con el fin de reducir las emisiones y mejorar la calidad del aire. Aunque muchas grandes ciudades han aplicado este método, los sistemas de control de acceso que implementan dichas zonas han levantado alarma social por su naturaleza intrusiva. Como consecuencia, se han propuesto sistemas que respetan la privacidad de los usuarios siempre que estos se comporten honestamente. No obstante, esto abre las puertas a ataques de confabulación, como ataques de "relay", que pueden llevar a suplantar de identidad de usuarios. Para paliar esta problemática, este artículo propone un sistema de generación de pruebas distribuido basado en el entorno en el que los usuarios cercanos, de forma privada, acreditan entre sí su posición y sus tiempos de respuesta con el fin detectar un ataque de "relay". El conjunto de pruebas generadas permiten determinar cuándo las credenciales de un usuario están siendo transmitidas en tiempo real y determinar si dicho usuario está confabulado con el atacante, caso en el que es posible revocar su privacidad.**

***Index Terms*—LEZ (Low Emission Zones), Ciudades inteligentes (Smart Cities), Privacidad (Privacy), Seguridad (Security), Pruebas de localización (Location proofs), Ataques de "relay" (Relay Attacks).**

I. Introducción

Los altos niveles de contaminación ambiental, derivados en gran parte de la congestión de tráfico urbano, se han convertido en un grave problema para las grandes ciudades en todo el mundo. En los núcleos urbanos de estas grandes áreas metropolitanas, los niveles de contaminación superan con creces algunos de los límites establecidos por la Organización Mundial de la Salud [1] suponiendo un peligro para la salud de sus ciudadanos. Para abordar este problema, las administraciones gubernamentales han empezado a aplicar medidas para fomentar un uso racional de vehículos, que incluyen, entre otros, restricciones en la circulación de vehículos contaminantes, carriles para vehículos de alta ocupación (VAO) o la delimitación de zonas de bajas emisiones (LEZ).

De entre las mencionadas, la implantación de LEZs, que consiste en un área donde se aplican restricciones o peajes a sus usuarios de acuerdo con las emisiones de sus vehículos, es una de las medidas que más ha proliferado. Suecia, Italia, Holanda, Reino Unido o Alemania son ejemplos de países que implementan este tipo de zonas en sus grandes ciudades. Ante esta tendencia, surge la necesidad de implementar sistemas de control de acceso a las LEZ que permitan gestionar las restricciones o peajes a los que deben someterse los vehículos que circulan por estas zonas. El caso más citado en la literatura es, sin duda, la LEZ de Londres y su controvertido sistema de control [2]. Una red integrada por más de 300 cámaras es el que compone la columna vertebral de dicho sistema, cuyo fin consiste en fotografiar indiscriminadamente las matrículas de todos los vehículos que circulan por su interior, para posteriormente identificar si dichos vehículos abonan sus correspondientes tasas.

Sistemas de cariz tan invasivo como el mencionado han propiciado la aparición de propuestas diseñadas en torno a la privacidad de los usuarios. Sistemas de control de acceso como los presentados en [3], [4] promueven respetar la privacidad de los usuarios en todo momento, y solo revocarles ese derecho en el momento en que se comportan de forma deshonesta. De este modo, la matricula del vehículo solo es fotografiada en caso de que el usuario omita, total o parcialmente, el proceso de autenticación con la infraestructura de control de acceso del sistema.

El enfoque de privacidad revocable aplicado a los sistemas de control de acceso supone un gran aliciente para los usuarios de dichos sistemas, pero también abre nuevas vías de ataque en las que el usuario puede intentar suplantar a otros usuarios amparado por su anonimato. Este tipo de ataques cobran especial sentido en LEZs, donde los vehículos que menos contaminan tienen tasas más bajas o incluso nulas.

Esto puede llevar a usuarios a realizar acciones fraudulentas dirigidas a confabularse o suplantar a usuarios que dispongan de credenciales para vehículos de bajas emisiones.

Para evitar ataques basados en el robo de credenciales y posterior suplantación de los usuarios, los servicios basados en localización vehicular (VLBS) hacen uso de hardware específico a prueba de manipulaciones, como una unidad de a bordo (OBU) o similar.

No obstante, esta medida es insuficiente contra los ataques basados en la confabulación, en los cuales se suplanta la identidad de un usuario simplemente redireccionando los paquetes recibidos hasta el vehículo que se desea suplantar y reproduciendo sus respuestas. Por medio de este ataque de "relay" o baliza, se hace creer a la infraestructura del sistema que el vehículo suplantado se encuentra accediendo a la zona restringida cuando en realidad se encuentra en otro lugar. (ver Figura 1).

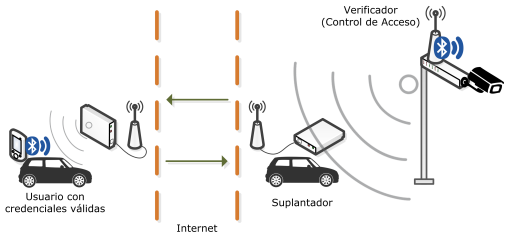

Figura 1. Ataque de baliza o "relay"

I-A. Contribución y organización del trabajo

Con la intención de abordar problemas todavía por resolver en la literatura actual, cuando no se puede asumir la integridad e irrefutabilidad de las ubicaciones de los dispositivos de localización, en este artículo afrontamos la problemática suscitada por el ataque de "relay" por medio de herramientas presentes en la literatura como pruebas de localización distribuidas y el análisis de tiempos de respuesta en las comunicaciones.

Con esto en mente, proponemos un nuevo sistema generador de pruebas distribuido, basado en el entorno y respetuoso con la privacidad de los usuarios, a partir de las cuales sea posible detectar un ataque de "relay". En dicho sistema, las entidades cercanas corroboran tanto la posición como los tiempos de respuesta de los usuarios con el fin de calcular un umbral del sobrecoste en la comunicación propio de un ataque de "relay". Las pruebas generadas actúan como garantía de que credenciales de un usuario no están siendo transferidas remotamente en tiempo real desde otra ubicación. Más concretamente, nuestras contribuciones son las siguientes:

- Proporcionar un sistema de generación de pruebas basado en el entorno cercano donde se respeta la anonimidad y privacidad de todos los usuarios implicados en el proceso. Las pruebas recolectan información sobre la posición y los tiempos de respuesta del entorno cercano con el objetivo de detectar comportamientos propios de un ataque de "relay".
- Permitir identificar al menos a uno de los usuarios que se han confabulado para perpetrar el ataque de "relay". Al generar pruebas que incluyen la ubicación, es posible determinar si el usuario que está siendo suplantado está confabulado con el atacante, en cuyo caso es identificado, o se trata de un usuario honesto víctima del ataque, con lo cual la prueba generada es desechada.

La contribución está organizada de la forma siguiente. En la Sección II se debate el estado actual de la literatura. En la Sección III se describe el modelo del sistema dando una visión general de la propuesta. La Sección IV contiene el protocolo en el que se basa el sistema presentado. La Sección V incluye un estudio del control de fraude de la propuesta. La Sección VI incluye un breve estudio sobre privacidad que ofrece el sistema. Finalmente, las conclusiones se presentan en la Sección VII.

II. Antecedentes

El uso de pruebas de localización o basadas en el entorno, que garantice la irrefutabilidad e integridad de las ubicaciones de los usuarios, es una estrategia que ya se ha considerado previamente en una gran cantidad de entornos sujetos a este tipo de servicios.

Este procedimiento, no obstante, abre gran número de cuestiones en relación a la seguridad y privacidad de los usuarios. Esto se debe a que, por un lado, es necesario garantizar la autenticidad de la prueba de localización vinculándola con la identidad del usuario. Por el otro, dicho vínculo puede revelar la localización del usuario a más partes del sistema de las requeridas. En los últimos años, numerosos trabajos se han hecho eco de esta situación y han presentado diferentes propuestas [5], [6], [7], [8], [9], [10] intentando abordar dicha problemática.

Las propuestas existentes pueden englobarse en dos grupos atendiendo a que entidad es la encargada de generar las pruebas de localización. En los trabajos [5], [6], [7] la generación de dichas pruebas es centralizada y recae sobre la infraestructura del sistema que actúa como autoridad de localización. Esto supone que las pruebas solo pueden generarse en puntos muy concretos lo cual limita su usabilidad.

En el segundo grupo, las propuestas [8], [9], [10] optan por un método de generación distribuida, las cuales se sustentan del entorno más cercano al usuario para generar pruebas de localización de forma privada. En este tipo de esquemas, los elementos cercanos, como por ejemplo otros usuarios, son los que, en conjunto, comprueban y generan las pruebas de localización. Aunque esta solución es más práctica que la centralizada, su naturaleza ocasiona nuevos problemas relacionados con la privacidad y la seguridad, ya que no se puede garantizar la honestidad de las entidades que generan las pruebas.

Para abordar esta problemática, en [8] se presenta un sistema basado en coartadas que permite que los móviles ubicados en una determinada área, llamados testigos, generen conjuntamente pruebas de localización de un dispositivo cercano. La identidad del usuario se mantiene oculta por medio de esquemas de compromiso criptográficos y solo es revelada en el momento de verificar la prueba. En [9] se presenta el sistema APPLAUS, que propone el mismo principio en la generación de pruebas de localización, pero usando pseudónimos que cambian periódicamente para conservar la privacidad de los usuarios. Además aborda problemas de confabulaciones entre usuarios y múltiples niveles de granularidad en la ubicación que no se consideraban en [8]. Mejoras sobre la detección de confabulaciones entre usuarios es lo que reivindica [10]. En este trabajo los autores presentan el sistema STAMP, al que integran un protocolo de límite de distancia con el fin de detectar usuarios que intenten generar pruebas remotamente.

Todos los sistemas anteriormente mencionados parten de la premisa que el usuario es el interesado en probar su localización, ya que en el entorno donde se integren dichos sistemas el usuario será recompensado de alguna forma al demostrar donde se encuentra físicamente. Ante este escenario, situaciones como intentar pasar inadvertido o suplantar a otro usuario ante la infraestructura del sistema, como sucede en un sistema de control de acceso a una LEZ, carecen de sentido y, por tanto, ninguno de los sistemas mencionados plantea o resuelve dichas cuestiones.

III. Modelo del Sistema

Nuestra propuesta plantea un nuevo sistema generador de pruebas basadas en el entorno cercano que permite detectar comportamientos propios de un ataque de "relay" a partir de la información que estas contienen. Aunque el esquema presentado en este artículo está orientado hacia un ámbito vehicular, como por ejemplo las LEZs, nuestro sistema generador de pruebas puede ser extrapolado a cualquier escenario donde se requiera controlar el acceso a un área restringida.

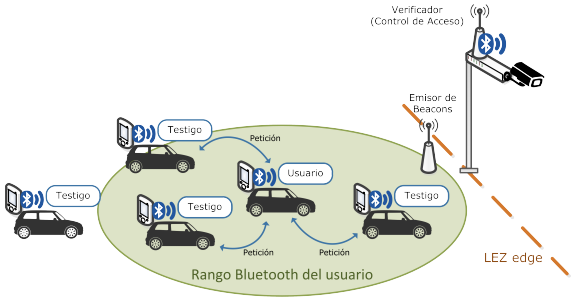

Figura 2. Arquitectura del sistema

La Figura 2 muestra un esquema general del sistema propuesto en este artículo. Se asume que los vehículos, tanto los que solicitan como los que generan pruebas, tienen integrado un dispositivo capaz de comunicarse inalámbricamente (p.e. Bluetooth o WIFI), de obtener su ubicación y conectarse a Internet en momentos puntuales.

Cuando un vehículo se acerca al Control de Acceso (CdA) de una zona restringida, una etiqueta BLE despierta al dispositivo encargado de ejecutar el protocolo. En ese momento se inicia la construcción de sus pruebas solicitando al resto de usuarios, dentro del alcance de su dispositivo de comunicación inalámbrica, la generación de una prueba. Para ello establece una comunicación segura con los usuarios dentro de su alcance para que individualmente acrediten su posición y sus tiempos de respuesta durante las comunicaciones. Cada uno de estos usuarios actúa como testigo, comprueba si la información que ha recibido es coherente con la suya y, en caso afirmativo, responde con una prueba criptográfica que lo corrobora. El conjunto de pruebas recibidas de todos los testigos integran la coartada del usuario con la que es posible demostrar su ubicación y que no está transmitiendo sus credenciales mediante la confabulación con otros usuarios.

En el momento de acceder a la zona restringida, el usuario transmite esta coartada al CdA que actúa como verificador. El CdA comprueba la validez de la coartada del usuario verificando cada una de las pruebas que le han generado el resto de usuarios. Si todas las pruebas son válidas, se asume que la coartada es válida y que el usuario está siendo honesto. En caso contrario, el CdA tomará las medidas pertinentes para revocar el anonimato del usuario en cuestión.

Durante este proceso, gracias a la generación basada en el entorno y en base a la información contenida en las coartadas, el CdA es capaz de generar temporalmente un mapa de los pseudónimos de usuarios que se encuentran en sus cercanías. Este mapa no solo determina las interacciones entre pseudónimos sinó que, debido a que las pruebas contienen información sobre ubicación y tiempo, también determina la distancia física y el tiempo de respuesta entre ellos.

Teniendo en cuenta que para perpetrar un ataque de "relay" hace falta un atacante que actúe de baliza y retransmita las señales Bluetooth hasta el usuario a suplantar, el CdA, gracias al mapa generado, calcula el umbral del tiempo de respuesta a partir del cual el sobrecoste de comunicación indica que hay una retransmisión de paquetes propia de un ataque de "relay". En base a esto también toma las medidas pertinentes para revocar la privacidad de los usuarios implicados.

IV. Descripción del Protocolo

En esta sección en primer lugar se describe de forma breve los actores, y a continuación las fases o operaciones que se pueden dar en el sistema.

IV-A. Actores

Nuestro sistema está compuesto por cuatro entidades: i) demostrador, ii) testigos, iii) Verificador y iv) Autoridad Certificadora.

- El demostrador (D) es un usuario del sistema (conductor) que dispone de un dispositivo, como una OBU, con GPS integrado que obtiene pruebas de su entorno cercano para demostrar su ubicación y tiempos de respuesta con dicho entorno a una tercera parte. En el escenario que proponemos D sería cualquier conductor que accede a una LEZ o zona de acceso restringido.
- El testigo (T) es otro usuario del sistema, con un dispositivo que integra GPS, que genera y avala pruebas de un D próximo físicamente cuando este lo solicite.
- El verificador (V) es la entidad que verifica las coartadas que presentan los Ds. En nuestro escenario, V sería la infraestructura que controla el acceso a la LEZ y que, en el momento en que un vehículo acede a la zona restringida, verifica que usuario no está transfiriendo sus credenciales en tiempo real por medio de un ataque de "relay".
- La Autoridad certificadora (AC) es una institución dedicada a generar y gestionar los materiales criptográficos a todas las entidades implicadas, p.e. claves públicas/privadas, certificados y pseudónimos.

IV-B. Fases

Las fases u operaciones que se realizan en el sistema propuesto son las siguientes: i) Inicialización; ii) Generación de pruebas; iii) Verificación; y iv) Control del Fraude.

IV-B1. Inicialización: Durante la fase de inicialización la AC genera y provee al resto de entidades que participan en el protocolo de los elementos criptográficos requeridos.

- Cada V con identificador ID_V consigue una clave privada sk_V, una clave pública pk_V y su correspondiente certificado $Cert_V^{AC}$.
- El dispositivo de cada usuario, independientemente del rol que desempeña como D o T, establece una conexión segura con la AC y recibe un pseudónimo PS_D, una clave privada sk_D, una clave pública pk_D y su correspondiente certificado $Cert_D^{AC}$. Dicho certificado solo contiene PS_D en el campo CommonName para evitar la identificación del usuario. Cada cierto intervalo

de tiempo, definido por el usuario, vuelve a repetirse este proceso a fin de generar un nuevo pseudónimo para el usuario. Una vez el usuario ha recibido sus nuevas claves y certificados, las anteriores son revocadas.

IV-B2. Generación de pruebas: La fase de generación de pruebas comienza en el momento en que un usuario requiere que su entorno cercano confirme su ubicación. El primer paso para iniciar el proceso es obtener un token del entorno que V emite periódicamente. Para ello V realiza las siguientes operaciones:

- Genera un token donde $V_{token} = \{ID_V, t_0, t_f\}$. Donde ID_V es el identificador de V, t_0 y t_f son timestamps que determinan el periodo de validez del token.
- Firma digitalmente el token $Sig^V(V_{token})$
- Emite V_{token} y $Sig^V(V_{token})$ periódicamente hasta la generación de un nuevo token.

Cuando un usuario D capta una emisión de V_{token} puede iniciar la construcción de sus pruebas basadas en entorno, para ello realiza el siguiente proceso:

- Verifica la firma $Sig^V(V_{token})$ y comprueba que el token no haya expirado.
- Enmascara su posición inicial $PosI_D$ en $\rho = Hash(PosI_D)$, donde $Hash$ es una función criptográfica de digest considerada segura.
- Construye una petición de generación de pruebas $D_{req} = \{V_{token}, \rho, t_1\}$. Donde t_1 es el timestamp del momento en que se genera la petición.
- Firma digitalmente los datos a enviar $Sig^D(D_{req})$.
- Hace un broadcast de D_{req} y $Sig^D(D_{req})$.

Cada T que recibe la petición D_{req} puede generar una prueba para D. Para ello realiza las siguientes operaciones:

- Verifica la firma digital de $Sig^D(D_{req})$ contenido en D_{req}.
- Verifica que los timestamps en D_{req} son consistentes. Para ello verifica que $t_0 < t_1 < t_2 < t_f$, donde t_2 es el timestamp del instante actual. Si la verificación no es correcta el proceso se detiene y T no responde a D.
- En caso afirmativo, genera una prueba $T_{res} = \{D_{req}, Pos_T, t_2\}$, donde Pos_T es la posición actual de T, y la firma digitalmente $Sig^T(T_{res})$.
- Envía T_{res} y $Sig^T(T_{res})$ a D.

Para cada prueba que recibe D, comprueba y almacena T_{res} realizando los siguientes pasos:

- Verifica la firma digital $Sig^T(T_{res})$.
- Verifica si la información contenida en T_{res} es coherente. Para ello comprueba que el D_{req} recibido coincide con el enviado, que Pos_T esté en un área cercana la posición actual de D $PosF_D$ y que $t_0 < t_1 < t_2 < t_3 < t_f$. Siendo t_3 la marca temporal actual. En caso que alguna de estas verificaciones falle, D desecha la prueba.
- Si las anteriores verificaciones son correctas, D almacena, junto al resto de pruebas derivadas de la misma petición D_{req}, la prueba recibida como $PR_i = \{PosI_D, PosF_D, Pos_T, t_2, t_3, Sig^T(T_{res})\}$.

IV-B3. Verificación: Cuando D se encuentra dentro del radio de comunicación de V, establece una comunicación segura e inicia la transmisión de las pruebas obtenidas. Para ello D realiza las siguientes operaciones:

- Recupera todas las pruebas PR_i a una petición D_{req}.
- Construye la prueba $D_{proof} = \{D_{req}, PR_1|...|PR_i\}$ y la firma digitalmente $Sig^D(D_{proof})$.
- Envía a V D_{proof} y su firma $Sig^D(D_{proof})$.

Cuando V recibe una coartada de un D comprueba la validez de la misma realizando los siguientes pasos:

- Verifica la firma de $Sig^D(D_{proof})$.
- Verifica si V_{token} se corresponde con el que estaba emitiendo durante t_0 y no ha expirado.
- Verifica la validez de cada prueba PR_i contenida en D_{proof}:
  - Verifica la firma $Sig^T(T_{res})$ con la información contenida en PR_i y D_{req}.
  - Comprueba que el pseudónimo PS_T contenido en el certificado de T es único en la actual D_{proof}
  - Calcula $Hash(PosI_D)$ y verifica que es igual a ρ contenido en D_{req}.
  - Comprueba que $PosI_D$, $PosF_D$ y Pos_T están contenidos en una área cercana a V.
  - Comprueba que los tiempos son coherentes y cumplen $t_0 < t_1 < t_2 < t_3 < t_f$.
- Si las comprobaciones son correctas se acepta PR_i como prueba válida. En caso contrario se descarta.

Si un determinado número de pruebas pasan estas verificaciones, la coartada D_{proof} se considera válida y se almacena. El umbral que determina cuantas pruebas son necesarias es dinámico y lo determina V en función del tráfico o de la frecuencia de accesos en ese momento.

IV-B4. Control del Fraude: A partir de las coartadas D_{proof} válidas almacenadas, V construye un mapa de interacciones entre pseudónimos. Por cada prueba PR_i contenida en D_{proof} realiza los siguientes pasos:

- Añade una arista en el mapa entre los pseudónimos de D PS_D y T PS_T.
- Calcula las distancias entre D y T usando $PosI_D$, $PosF_D$ y Pos_T.
- Calcula el tiempo de respuesta entre D y T a partir de t_1, t_2 y t_3. En base a esto, comprueba si el tiempo de respuesta supera la media de tiempo para generar una prueba para la distancia física entre D y T.
- Si el tiempo supera un umbral sobre la media se añade una incidencia en la arista del mapa entre PS_D y PS_T.

Periódicamente, V comprueba las relaciones entre los diferentes pseudónimos en el mapa. En el momento que un PS concentra una cierta cantidad de incidencias en una proporción elevada de sus relaciones en el mapa se le puede acusar de fraudulento. De la misma forma, también verifica que cada PS tenga más de una arista con otros pseudónimos, es decir, que haya generado pruebas como T además de presentar su D_{proof}. Si se detecta un PS egoísta que no ha generado pruebas para otros usuarios también se le acusa de fraude. En ambos casos V toma las medidas pertinentes e informa a AC para que revoque la privacidad del usuario implicado.

V. Estudio del Control de Fraude

En esta sección se definen los distintos ataques de "relay" que pueden darse en el entorno vehicular propuesto en este artículo. Para cada escenario se detalla cómo se defiende del

ataque el protocolo propuesto y cómo reacciona ante posibles contramedidas de los atacantes.

V-1. Caso normal: En la Figura 3 se muestra la generación de una prueba, por parte de un T honesto, para un usuario D en condiciones normales y sin que se produzca ningún ataque durante el proceso.

Figura 3. Caso normal

En este escenario, D, en el instante t_1, solicita la generación de una prueba. T recibe esta petición y entre los instantes t_2 y $t_{2'}$ genera la prueba con un timestamp t_2 y una posición Pos_T. Este tiempo de cómputo puede considerarse como negligible en comparación con el coste temporal de las comunicaciones Bluetooth de acuerdo con los estudios presentados en [4]. D completa la generación de la prueba añadiendo el instante de recepción t_3 y su posición final $PosF_D$.

Al no haber interferencias derivadas de actividades de usuarios deshonestos, el coste temporal de la generación de una prueba se obtiene de $t_3 - t_1$. V realiza este cálculo para cada prueba contenida en las coartadas que envían los Ds, con el fin de mantener una media actualizada del tiempo que les cuesta a los Ts responder con una prueba T_{res} a una petición D_{req}. Esta media se calcula para distintos rangos de distancias entre T y D para tener en cuenta el impacto de la distancia en la potencia de señal de las comunicaciones inalámbricas. V puede realizar estos cálculos porque todas las pruebas contienen $PosI_D$, $PosF_D$ y Pos_T. Estas medias sirven como referencia para detectar sobrecostes de comunicación que puedan indicar que se está cometiendo fraude por medio de un ataque de relay. Se asume que este tipo de ataques son casos excepcionales y que este tipo de procedimiento representa un porcentaje muy bajo del total de las pruebas que se generan.

V-2. Suplantación de T: En el escenario ilustrado en la Figura 4, un atacante (AT) confabulado con un T deshonesto, en una ubicación arbitraria, generan una prueba por medio de un ataque de "relay" para la coartada de D. Dichos actores se describen a continuación:

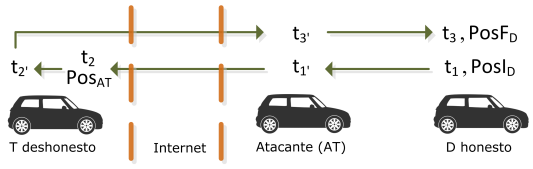

Figura 4. Ataque con suplantación de T

- D honesto con credenciales válidas que realiza una petición legítima a su entorno cercano para obtener una coartada.
- Un AT con la capacidad de hacer un ataque de "relay" para suplantar a un T deshonesto con el cual está confabulado. AT no tiene por qué ser usuario del sistema ni disponer de credenciales.
- Un T deshonesto, confabulado por con el atacante, que dispone de credenciales válidas.

Como puede apreciarse en la Figura 4, D en el instante t_1 emite una petición D_{req} para generar una coartada. AT, que retransmite las señales Bluetooth hacia T, recibe esta petición en el instante $t_{1'}$ y la envía a T que la recibe en t_2. En ese instante, T genera la prueba utilizando la posición Pos_{AT} del atacante en vez de la suya para evitar delatar el ataque de "relay". En $t_{2'}$ T inicia la transmisión de la prueba T_{res} hacia D repitiendo el proceso en sentido inverso y usando AT como baliza. D cierra la generación de la prueba añadiendo t_3 y su posición final $PosF_D$.

En el esquema descrito puede apreciarse que al ejecutar el ataque existe un sobrecoste debido a la comunicación extra entre AT y T. Este sobrecoste viene definido por $(t_2 - t_{1'}) + (t_{3'} - t_{2'})$ y representa el tiempo extra sobre el caso honesto descrito en la Sección V-1 que V valora para detectar un ataque de "relay".

Ante esta situación, T solo tiene maniobra para modificar el t_2 que incluye en T_{res}. No obstante, falsear dicho tiempo no tiene ninguna implicación en el tiempo de total de comunicación determinado por $t_3 - t_1$, ya que ambos valores son fijados por D que es honesto.

V-3. Suplantación de D: La Figura 5 muestra un escenario donde un D deshonesto, situado en una ubicación arbitraria, genera una coartada para un AT por medio de un ataque de "relay". Intervienen los siguientes actores:

- Varios Ts honestos que generan pruebas para un D cuando este lo solicita.
- Un AT con la capacidad de hacer un ataque de "relay" para suplantar a un D deshonesto con el cual está confabulado. AT no tiene por qué ser usuario del sistema.
- Un D deshonesto, confabulado con el atacante, que dispone de credenciales válidas.

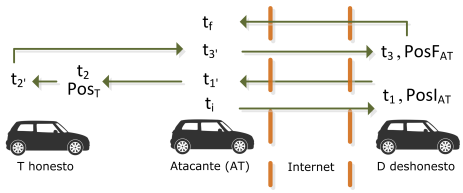

Figura 5. Ataque con suplantación de D

Como se puede ver en la Figura 5, el proceso lo inicia AT cuando en t_i envía V_{token} a D, quien se encuentra fuera del alcance de V y Ts. En t_1, D inicia el protocolo generando la petición D_{req}, usando la $PosI_{AT}$ para no delatar el ataque, y la envía a AT para que haga un broadcast a los Ts que le rodean. Cada T genera una prueba T_{res} en el instante t_2 y envía su respuesta a AT. AT de nuevo actúa de baliza y, en $t_{3'}$, envía a D las T_{res} que recibe junto con $PosF_{AT}$. Para cada prueba T_{res}, D introduce el tiempo de recepción t_3 y la nueva posición de AT. Finalmente construye D_{proof} con todas las pruebas recibidas. El proceso termina en t_f cuando AT recibe la D_{proof} y la envía a V haciéndose pasar por D.

En este escenario el ataque para suplantar a D también presenta un coste extra de comunicación. De acuerdo con la Figura 5, este sobrecoste se produce a causa de la comunicación extra entre AT y D y ahora se define por $(t_{1'} - t_1) + (t_3 - t_{3'})$. Hay que destacar que los costes de comunicación $(t_1 - t_i)$ y $(t_f - t_3)$ no pueden considerarse para detectar una suplantación de D, ya que $(t_1 - t_i)$ se produce antes de iniciar la construcción de la coartada y $(t_f - t_3)$ después de finalizarla. Aunque los tiempos que intervienen son distintos, el coste extra derivado del ataque en este caso es equivalente al de V-2. Esto es debido a que durante el ataque se envía la misma información entre D y T. Si bien es cierto que se genera una prueba por cada T, estos procesos son simultáneos e independientes.

Aunque queda patente que existe un sobrecoste de comunicación, D, en este caso, tiene capacidad para modificar los tiempos t_1 y t_3 que incluye en su D_{proof}. Si AT, con el que está confabulado, le facilita los tiempos t_i y $t_{3'}$, D puede calcular fácilmente el tiempo extra de comunicación y modificar los timestamps t_1 y t_3 para que el ataque de "relay" no pueda ser detectado por medio del tiempo de respuesta.

Aunque con este mecanismo D puede evitar ser detectado a partir de su D_{proof}, D seguirá interpretando el rol de T y generando pruebas T_{res} para otros usuarios. Ante esto, queda claro que las D_{proof} de los otros usuarios honestos acabaran delatando el ataque de "relay". Llegado a este punto, un usuario fraudulento puede evitar generar pruebas para otros usuarios a fin de no ser detectado. No obstante, el protocolo también considera fraudulento este comportamiento e igualmente emprende acciones contra el usuario.

Después de analizar los 3 escenarios posibles puede concluirse que, aunque los atacantes disponen de medios para intentar ocultar el sobrecoste de comunicación en ciertos casos, no tienen alternativa cuando generan pruebas como testigos para otros usuarios. Esto, sumado al hecho de que se considera fraudulentos a los usuarios egoístas que no colaboran en la generación de pruebas, garantiza que, con el protocolo propuesto, es posible registrar con seguridad el tiempo extra que consume un ataque de "relay".

VI. Privacidad

El sistema propuesto evita metodologías invasivas para la privacidad como el uso de cámaras para verificar la ubicación de los usuarios en el momento de acceder a una zona restringida. En vez de eso, el sistema hace uso del entorno cercano para generar pruebas firmadas criptográficamente que permitan verificar que sus credenciales no están siendo transferidas en tiempo real por medio de un ataque de "relay". Al usar esquemas de clave asimétrica que implican el uso de certificados que identifican al usuario, la privacidad de estos se protege por medio del uso de pseudónimos cuya relación con la identidad usuario solo la AC conoce. En el caso de los certificados, la AC los emite especificando únicamente el pseudónimo en el campo CommonName. Para evitar que un atacante o entidad del sistema pueda vincular un pseudónimo con su propietario, un usuario puede configurar cuando quiere solicitar un nuevo certificado y revocar el anterior; acto que conlleva la regeneración de sus claves. Finalmente, la inclusión de la posición de los usuarios en las pruebas que genera el sistema no tiene implicaciones para su privacidad. Esto se debe a que la generación de las mismas solo se produce durante los accesos y salidas de las zonas restringidas y por tanto no expone la ruta de los usuarios implicados.

VII. Conclusiones

El sistema propuesto permite generar pruebas, de forma privada, en colaboración con el entorno cercano para detectar ataques de "relay". La información sobre la posición y los tiempos de respuesta que contienen dichas pruebas garantiza que al menos a uno de los usuarios confabulados en el ataque pueda ser identificado y señalado como culpable. Más allá del entorno vehicular, la propuesta podría extrapolarse a cualquier entorno donde se detecte la necesidad de regular la entrada y salida de usuarios. Finalmente, el estudio de control de fraude realizado concluye que resulta imposible para un usuario deshonesto ocultar los indicios del ataque y que, por tanto, el sobrecoste que este produce en las comunicaciones siempre queda reflejado en las pruebas que se generan. Actualmente se está desarrollando el sistema que permita evaluar el verdadero alcance del sobrecoste derivado de un ataque de "relay" y poder verificar su aplicación en un entorno real. Debido al espacio disponible se ha dejado como trabajo futuro un estudio detallado de la seguridad y la privacidad que ofrece la propuesta.

Agradecimientos

This work was partially supported by the DGT under the project ISSUM SPIP2017-02250 and the Spanish Government under SmartGlacis TIN2014-57364-C2-R and Red de excelencia Consolider ARES TIN2015-70054-REDC projects. Some of the authors are members of the UNESCO Chair in Data Privacy, yet the views expressed in this paper neither necessarily reflect the position of the UNESCO nor commit with that organization.

Referencias

[1] World Health Organization. Air quality guidelines: global update 2005: particulate matter, ozone, nitrogen dioxide, and sulfur dioxide. World Health Organization, 2006.

[2] G. Santos. Urban congestion charging: A comparison between London and Singapore. Transport Reviews 25 (5), 2005, pp. 511-534.

[3] J. Castella-Roca, M. Mut-Puigserver, M. Payeras-Capella, A. Viejo and C. Angles-Tafalla. Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas. In Computer Communication and Networks (ICCCN), 2017, 26th International Conference on IEEE.

[4] C. Angles-Tafalla, J. Castella-Roca, M. Mut-Puigserver, M. Payeras-Capella and A. Viejo. Secure and Privacy-Preserving Lightweight Access Control System for Low Emission Zones. To be accepted in Computer Networks.

[5] Saroiu, Stefan, and Alec Wolman. Enabling new mobile applications with location proofs. Proceedings of the 10th workshop on Mobile Computing Systems and Applications. ACM, 2009.

[6] Luo, W., and U. Hengartner. Veriplace: a privacy-aware location proof architecture. Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems. ACM, 2010.

[7] Zhang, Y., Tan, C. C., Xu, F., Han, H., and Li, Q. Vproof: Lightweight privacy-preserving vehicle location proofs. IEEE Transactions on Vehicular Technology 64.1 (2015): 378-385.

[8] Davis, Benjamin, Hao Chen, and Matthew Franklin. "Privacy-preserving alibi systems."Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.

[9] Zhu, Zhichao, and Guohong Cao. Toward privacy preserving and collusion resistance in a location proof updating system. IEEE Transactions on Mobile Computing 12.1 (2013): 51-64.

[10] Wang, X., Pande, A., Zhu, J., and Mohapatra, P. STAMP: enabling privacy-preserving location proofs for mobile users. IEEE/ACM transactions on networking 24.6 (2016): 3276-3289.