(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 704 467**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 8/16 (2009.01)
H04L 29/06 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.10.2013 E 13005086 (7)**

(97) Fecha y número de publicación de la concesión europea: **10.10.2018 EP 2866484**

(54) Título: **Un método para anonimizar los datos recopilados dentro de una red de comunicación móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2019

(73) Titular/es:

TELEFÓNICA GERMANY GMBH & CO. OHG (100.0%)
Georg-Brauchle-Ring 23-25
80992 München, DE

(72) Inventor/es:

UKENA, JONATHAN y
SCHÖPF, PHILIP

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Un método para anonimizar los datos recopilados dentro de una red de comunicación móvil

La invención se refiere a un método para anonimizar datos de eventos recopilados dentro de una red y a un método para anonimizar datos de relaciones con clientes de una red de comunicación móvil.

Los operadores de sistemas o redes arbitrarios, es decir, que se aplican en el sector bancario, el sector de la salud pública, el sector de las telecomunicaciones, etc., registran datos relacionados con los clientes, tales como información personal sobre sus clientes, detalles de contacto y, opcionalmente, información del contrato. Por ejemplo, los datos incluyen atributos relacionados con el nombre del abonado, la dirección, la fecha de nacimiento, los datos bancarios y muchos más. La recopilación de estos datos es necesaria para fines de administración, facturación o para mantener disponible para las autoridades. A continuación, dichos datos se definen como datos de relación con el cliente (CRM) o datos estáticos.

Además, dichos sistemas/red podrían recopilar continuamente datos adicionales durante la operación regular del sistema/red. La generación de los llamados datos de eventos se desencadena por la actividad del abonado que genera un determinado evento dentro del sistema o por el propio sistema. Un conjunto de datos de eventos incluye varios atributos que describen diferentes propiedades del evento desencadenado, por ejemplo, una marca de tiempo, tipo de evento, etc. Estos conjuntos de datos de eventos están asociados con un identificador personal que permite la asignación del conjunto de datos de eventos generados a un cliente individual del sistema/red.

Una aplicación particular de dicho sistema es un sistema de comunicación móvil que permite la comunicación entre dos o más abonados. Los operadores de sistemas de comunicación registran datos relacionados con el abonado, tales como información personal sobre los abonados, detalles de contacto e información del contrato. Por ejemplo, los datos incluyen atributos relacionados con el nombre del abonado, la dirección, la fecha de nacimiento, los datos bancarios y muchos más. La recopilación de estos datos es necesaria para fines de facturación o para que estén disponibles para las autoridades. A continuación, dichos datos se definen como datos de relación con el cliente (CRM) o datos estáticos.

A medida que los conjuntos de datos de eventos, los proveedores de la red recolectan continuamente datos adicionales llamados datos de eventos de ubicación durante el funcionamiento normal de la red. Cada conjunto de datos de eventos de ubicación está relacionado con un evento específico de un abonado individual. Los eventos pueden ser activados por un abonado/usuario, la red o un dispositivo que no es importante para su posterior procesamiento. El conjunto de datos incluye varios atributos, como un atributo de evento que describe el tipo de evento, uno o más atributos de ubicación que identifican la ubicación geográfica donde el abonado activó dicho evento y una marca de tiempo que define la hora del evento. Estos conjuntos de datos de eventos de ubicación están asociados con un identificador personal que permite la asignación del conjunto de datos de eventos de ubicación a un abonado individual del sistema de comunicación.

Debido a la retención de esta información, tales sistemas/redes, en particular los sistemas de comunicaciones móviles, ofrecen la posibilidad de proporcionar información sobre los hábitos del abonado, en particular con respecto a los datos de ubicación durante un intervalo de tiempo definido. Estos datos pueden usarse para crear perfiles de ubicación para sitios geográficos o para derivar patrones dinámicos de movimiento de masas. En este contexto, la información podría ser útil para una amplia gama de aplicaciones en el área de servicios de tráfico, servicios de ciudades inteligentes, servicios de optimización de infraestructura, servicios de información minorista, servicios de seguridad y muchos más. Por lo tanto, es deseable proporcionar la información generada en forma adecuada a las partes que se benefician de aplicaciones como las mencionadas anteriormente. Tales partes podrían incluir consejos locales, empresas de transporte público e infraestructura como proveedores de transporte público o proveedores de electricidad, minoristas, organizadores de eventos importantes u organismos de seguridad pública y muchos más usos y usuarios aún desconocidos.

Sin embargo, es obligatorio proporcionar esta información de forma anónima para proteger la privacidad de cada individuo, en particular de cada cliente/abonado del sistema o red de comunicación móvil. En consecuencia, el proveedor del sistema/red de comunicación móvil que suministra los datos solo debe proporcionar información extraída de datos anónimos y agregados sin revelar información personal. La divulgación de cualquier información personal está estrictamente prohibida, y en cualquier circunstancia debe evitarse el seguimiento y la identificación de personas.

Un atacante potencial puede identificar al abonado de los datos de eventos de ubicación generados simplemente observando al abonado y un evento observable que sea detectable para un observador debido a las acciones del propio abonado. Además, si muy pocos abonados de una red de comunicaciones móviles desencadenan la generación de datos de eventos de ubicación en una pequeña área geográfica, el único abonado puede ser identificado por dicha pequeña área geográfica; por ejemplo, si dicha área caracteriza su lugar de vida o trabajo.

Es una objeción de la invención proporcionar un método para la anonimización de los datos recopilados o utilizados dentro de un sistema o red arbitrarios, por ejemplo, una red de comunicación móvil, y cada uno de ellos está relacionado con un cliente/abonado individual de la red de sistemas/comunicaciones móviles.

El objeto mencionado anteriormente se resuelve mediante un método de acuerdo con la combinación de características de la reivindicación 1. Las realizaciones preferidas son objeto de las reivindicaciones dependientes 2 a 7.

Un método para anonimizar los datos de eventos recopilados dentro de un sistema o red que proporciona un servicio para abonados/clientes en el que cada conjunto de datos de eventos está relacionado con un abonado/cliente individual del sistema/red e incluye al menos un atributo en el que el método cuenta el número de conjuntos de datos de eventos relacionados con diferentes abonados individuales que tienen valores idénticos o casi idénticos para al menos un atributo. Se debe tener en cuenta que el atributo de expresión se usa en el término de una propiedad específica del evento. El atributo puede representar una determinada categoría que puede tener un cierto valor. Por ejemplo, un atributo de evento puede tomar diferentes valores que definen diferentes tipos de eventos.

Cada conjunto de datos de eventos consta de uno o más atributos, por ejemplo, que contienen la hora en que se produjo un evento, pero también pueden contener información sobre el tipo de evento. Cada conjunto de datos de eventos está relacionado con un cliente individual del sistema, en particular asociando el conjunto de datos con un identificador personal, específicamente con un identificador personal anonimizado.

Por lo tanto, cada conjunto de datos de eventos describe un evento individual que fue activado por un cliente específico del sistema/red. Para el almacenamiento y suministro de dichos datos recopilados, es obligatorio anonimizar suficientemente los datos para evitar cualquier identificación del cliente individual.

Por lo tanto, el método inventivo identifica ciertos valores de atributo con poca actividad. Es decir, el método inventivo cuenta el número de eventos que tienen los mismos valores o casi los mismos para al menos un atributo y que son activados por diferentes clientes. Cuanto menor sea el número de eventos desencadenados por diferentes clientes, mayor será el riesgo potencial de desanonimización, lo que significa que el número de clientes diferentes es significativo. Si la cantidad de clientes diferentes aumenta el esfuerzo para lograr una desanonimización, debe ser significativamente mayor que lo que se obtendrá.

En una realización preferida particular de la invención, el sistema/red es una red de comunicación móvil y los datos de eventos se refieren a un conjunto de datos de eventos recopilados dentro de la red de comunicaciones móviles. La red de comunicación móvil se puede realizar como una red de comunicación móvil de acuerdo con 2G, 3G o cualquier otro estándar de comunicación móvil. Adicional o alternativamente, la red de comunicación móvil se relaciona con una red de área de ubicación inalámbrica.

Cada conjunto de datos de eventos de ubicación consta de uno o más atributos que contienen al menos el momento en que tuvo lugar un evento, pero también puede contener información sobre el lugar o el tipo de evento en la red de comunicaciones móviles. Al menos otro atributo se indica como un atributo de ubicación que define la ubicación donde ocurrió el evento. En ese caso, el conjunto de datos de eventos se especifica como un conjunto de datos de eventos de ubicación. Cada conjunto de datos de eventos de ubicación está relacionado con un abonado individual de la red de comunicaciones móviles, en particular asociando el conjunto de datos con un identificador personal, específicamente con un identificador personal anónimo.

Por lo tanto, cada conjunto de datos de eventos de ubicación describe un evento individual que fue activado por un abonado específico de la red de comunicaciones móviles. Para el almacenamiento y el suministro de dichos datos recopilados, es obligatorio anonimizar suficientemente los datos para evitar cualquier identificación del abonado individual.

Por lo tanto, el método inventivo identifica ubicaciones con poca actividad. Es decir, el método inventivo cuenta el número de eventos que ocurren en un lugar determinado y que son activados por diferentes abonados. Cuanto menor sea el número de eventos desencadenados por diferentes abonados, mayor será el riesgo potencial de desanonimización, lo que significa que el número de abonados diferentes es significativo. Si el número de abonados diferentes aumenta el esfuerzo para lograr una desanonimización, debe ser significativamente mayor que lo que se obtendrá.

Por razones de conveniencia, los aspectos preferidos posteriores del método de la invención se describen sobre la base de un sistema de comunicación móvil y datos de eventos de ubicación como un cierto tipo de datos de eventos. Sin embargo, la presente invención no debe limitarse a esto.

El método preferentemente ejecuta la supervisión y el recuento durante un cierto intervalo de tiempo y, posteriormente, reinicia la supervisión y el recuento en un nuevo intervalo de tiempo.

En una realización preferida de la invención, el método descarta todos los conjuntos de datos de eventos de ubicación recolectados con eventos que ocurren en una determinada ubicación si el número contado de estos conjuntos de datos de eventos de ubicación relacionados con diferentes abonados es menor que un umbral definido después de un intervalo de tiempo definido. El umbral se definirá dinámicamente para lograr una buena relación entre el uso de los datos del evento de ubicación y la anonimización suficiente de los datos del evento de ubicación. Dicho umbral puede ser fijo, establecido según la situación o uso del usuario o establecido dinámicamente según otras reglas, requisitos de eventos.

Alternativamente, en un aspecto diferente del método inventivo, toda la información personalizada incluida en los conjuntos de datos de eventos de ubicación recopilados, en particular el identificador personal anonimizado, se puede eliminar si el número contado es menor que un umbral definido. Al descartar toda la información personalizada incluida en los conjuntos de datos de eventos de ubicación, no es posible distinguir si un cierto número de eventos ocurridos en una ubicación determinada ha sido activado por uno o más de un abonado.

En un aspecto preferido particular de la invención, el método fusiona los conjuntos de datos de eventos de ubicación recopilados de diferentes ubicaciones si el número de al menos una ubicación es menor que un umbral definido. Dicho enfoque preferido particular mantiene una relación entre diferentes conjuntos de datos. Contrariamente al enfoque mencionado, ahora se puede determinar si ciertos eventos en ciertos lugares han sido activados por diferentes abonados. Sin embargo, dicho enfoque preferido garantizará que los eventos en una determinada ubicación hayan sido activados por un número suficiente de abonados diferentes, evitando así un proceso fácil de desanonimización.

La fusión de los conjuntos de datos de eventos de ubicación de diferentes ubicaciones se puede realizar reemplazando los atributos de ubicación de dichos conjuntos de datos de eventos de ubicación por un atributo de ubicación generalizado. El número de conjuntos de datos de eventos de ubicación relacionados con los distintos abonados individuales se cuenta para una determinada ubicación en la que la ubicación puede definirse como una determinada área geográfica. La fusión de los conjuntos de datos de eventos de ubicación puede realizarse incrementando el área geográfica y/o aumentando el radio de dicha área geográfica y/o aumentando la imprecisión del área o la decisión de si ocurrió un evento con dicha área. Además, los diferentes atributos de ubicación que describen áreas geográficas adyacentes entre sí se pueden combinar en un área geográfica más grande que incluya áreas más pequeñas. Por lo tanto, los atributos de ubicación de los conjuntos de datos de eventos de ubicación combinados se reemplazan por dicha área geográfica más grande. También es posible combinar áreas geográficas congéneres que no están ubicadas adyacentes entre sí.

Al concentrar los conjuntos de datos de eventos de ubicación de ubicaciones adyacentes, aumenta el número de eventos relacionados con diferentes abonados. La fusión de ubicaciones adyacentes se repetirá hasta que el número de abonados individuales que activen los conjuntos de datos de eventos de ubicación supere el umbral definido. Se acepta una inexactitud limitada de la información de ubicación reemplazada debido a una anonimización más suficiente de los datos del evento de ubicación.

Es concebible que solo se combinen los conjuntos de datos de eventos de ubicación con un número contado de conjuntos de datos de eventos de ubicación por debajo del umbral definido. Sin embargo, si no se puede lograr el número deseado de conjuntos de datos de eventos de ubicación al fusionar solo dichas ubicaciones, también podría ser posible combinar una ubicación con un número de conjuntos de datos de eventos de ubicación por debajo del umbral definido con una ubicación con un número conjuntos de datos de eventos de ubicación que superan el umbral definido en el que las áreas fusionadas pueden estar debajo del umbral establecido, pero combinados lo superan.

La generación y recopilación de un conjunto de datos de eventos de ubicación es activada preferiblemente por un abonado individual que solicita un servicio específico de la red de comunicaciones móviles. Por ejemplo, solicitar un servicio puede incluir la transmisión de un mensaje corto (SMS, MMS), una llamada telefónica entrante y/o saliente, y el inicio de una sesión de datos o similar. Un evento que es activado indirectamente por el abonado, por ejemplo, es un proceso de transferencia conocido que también generará un conjunto de datos de eventos de ubicación. Un terminal de abonado también puede iniciar un proceso de posicionamiento por sí mismo, en particular basado en un receptor de GPS y activado por una aplicación de teléfono inteligente, pero también utilizando otros métodos de ubicación, como el uso de Wi-Fi o celdas de redes móviles, mediante actualizaciones periódicas de ubicaciones realizadas por la red o paginación activa por la red. Además, el terminal podría estar ubicado pasivamente en la red, por ejemplo, en función de la triangulación. Tales eventos también pueden generar datos de eventos de ubicación respectivos.

Los conjuntos de datos de eventos de ubicación incluyen un atributo de marca de tiempo que define la hora en que ocurrió el evento. En caso de un evento visual, un atacante potencial podría comparar el evento observado en el mundo real con los conjuntos de datos de eventos de ubicación disponibles. Si el evento observado coincide con una marca de tiempo y un tipo de evento disponibles dentro de un conjunto de datos de eventos de ubicación, el identificador personal anonimizado incluido se puede asignar a una determinada persona (aunque el identificador personal permanece anónimo/con hash) Por lo tanto, de acuerdo con un aspecto preferido de la invención, el atributo de marca de tiempo también está ofuscado, especialmente para los tipos de eventos observables, pero la ofuscación también es posible para eventos no observables.

En una realización preferida de la invención, la marca de tiempo se modifica redondeando la marca de tiempo o agregando un desplazamiento de tiempo que a su vez se puede establecer aleatoriamente. Por lo tanto, un atacante potencial no puede asociar un evento visible a un conjunto de datos de eventos de ubicación específicos con respecto a la marca de tiempo almacenada.

La presente invención también se refiere a un método para anonimizar datos estáticos relacionados con abonados individuales de una red de comunicaciones móviles.

De acuerdo con la invención, cada conjunto de datos estáticos, también anotados como datos de clase de cliente (CCD), consta de atributos diferentes que se refieren a la información personal sobre el abonado. Por lo tanto, la información contenida en un único conjunto de datos se define por la combinación de los diferentes atributos que se refieren a la información personal y otros atributos no personales. El método de la invención garantiza que el número de ocurrencias de conjuntos de datos con información personal idéntica (es decir, una combinación idéntica de atributos con información personal) es mayor que un umbral configurable. Esto se puede lograr mediante el uso de una implementación de anonimato k. La implementación general del anonimato k fue propuesta por P. Samarati y L. Sweeney. En este contexto, se hace referencia a P. Samarati y L. Sweeney, “Generalizing Data to Provide Anonymity When Disclosing Information”, Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of Database Systems, pp. 188, 1998 (ACM).

El documento de solicitud de patente DE102010047117 se refiere a la anonimización de los datos de eventos generados por los suscriptores de un sistema de comunicación móvil.

Documento con el título PrivacyGrid Supporting Anonymous Location Queries in Mbole Environment.

El documento de solicitud de patente WO2012/136245 se refería a la anonimización de los datos de prueba de accionamiento generados por los abonados de un sistema de comunicación móvil.

Las solicitudes de patente US2011/0010563 y EP1950684 se refieren a la anonimización de los datos de abonado. Por lo tanto, las características de la invención aplican el anonimato k para la anonimización de datos estáticos relacionados con suscriptores individuales de una red de comunicaciones móviles, ya sea mediante la supresión de valores de atributos particulares o mediante la generalización de valores de atributos, lo que efectivamente significa que los conjuntos de datos se transforman para contener información menos específica.

Por lo tanto, los valores de al menos un tipo de atributo se reemplazan por valores generales. La selección de atributos a generalizar, es decir, clasificados, puede considerarse en orden jerárquico, por ejemplo, la clasificación de todos los atributos con respecto a un tiempo se realiza al principio. Si no se cumple el requisito con respecto a la deanonimización, la clasificación se aplica a un tipo diferente de atributos, por ejemplo, relacionados con la ubicación o la información del evento. También es posible tener un orden jerárquico para la clasificación dentro de un determinado tipo de atributo. Por ejemplo, la inexactitud de la información de ubicación de un atributo de ubicación se incrementa en etapas. La información de ubicación puede ser proporcionada por un identificador de celda y reemplazada por un código postal de varios dígitos. Para aumentar aún más la imprecisión de dicha información de ubicación, el código postal puede reducirse a un número menor de dígitos.

El proceso de clasificación se realiza preferiblemente reemplazando un cierto atributo de dos o más conjuntos de datos estáticos con un atributo común generalizado. La etapa de clasificación se realiza, además, preferiblemente hasta que el número de conjuntos de datos estáticos de cada grupo exceda un umbral definido.

Es posible que al menos un atributo del conjunto de datos estáticos se relacione con el género o la fecha de nacimiento o la edad o la profesión o el lugar de residencia de un abonado individual de la red de comunicaciones móviles.

La clasificación se puede hacer generalizando varias fechas de nacimiento de diferentes abonados a un intervalo de tiempo específico que incluye las diferentes fechas de nacimiento. Además, el atributo que se refiere a la profesión de un abonado se reemplazará por un atributo que describe el sector industrial de las respectivas profesiones. Por ejemplo, los profesionales de la salud y las enfermeras se clasificarán como personas que trabajan en el sector de la salud.

La invención también se refiere a un sistema de comunicación como se define en la reivindicación 8 adjunta. Es obvio que el sistema de comunicación se caracteriza por las propiedades y ventajas de acuerdo con el método de la invención. Por lo tanto, una descripción repetida se considera innecesaria.

Otras ventajas y propiedades de la presente invención se describen sobre la base de dos realizaciones mostradas en las figuras. Las figuras muestran:

Figura 1: una vista general arquitectónica sobre el sistema que usa el filtrado de datos de eventos de ubicación de acuerdo con la invención,

Figura 2: una vista general arquitectónica sobre un sistema de acuerdo con la figura 1 y adicionalmente incluye el filtrado de datos estáticos,

Figura 3: vista general arquitectónica de las etapas del método básico del proceso de anonimización multinivel (MAP) y

Figura 4: un diagrama de flujo que muestra el proceso de filtrado de datos de eventos de ubicación.

La Figura 3 ilustra la idea fundamental de un proceso de anonimización multinivel (MAP). La idea básica de ese proceso de anonimización se relaciona con un procedimiento de anonimización de datos para permitir el uso masivo de datos de ubicación para aplicaciones de big data con total respeto de las normas europeas de protección de datos. Los datos de ubicación masiva serán recopilados por proveedores de redes de comunicación móviles o inalámbricas, así como proveedores que recopilan información que se basa en otras tecnologías de ubicación como GPS; Galileo, Glonass, Compass, redes de sensores, etc., que además pueden poseer información personal detallada y verificada sobre sus abonados. Además, los proveedores de redes móviles pueden extraer datos de eventos de ubicación de los abonados. La información anónima y agregada recopilada por los operadores de redes móviles puede proporcionar información interesante para diferentes aplicaciones de terceros.

Por ejemplo, los proveedores de redes móviles pueden proporcionar datos anónimos y agregados a los consejos locales, empresas de transporte público, combinadores de infraestructura, como proveedores de transporte público o proveedores de electricidad, minoristas, organizadores de eventos importantes de organismos de seguridad pública que utilizan dicha información para mejorar los procesos de toma de decisiones y otros usos aún desconocidos.

Sin embargo, es obligatorio cuidar la privacidad de cada abonado y la información personal del abonado. Al dividir el proceso en varias etapas del proceso que se ejecutan dentro de diferentes sistemas que, además, pueden estar ubicados en diferentes zonas de seguridad con derechos de acceso específicos o incluso en locales legales de entidades independientes, se evita la posibilidad de generar una tabla de asignación entre identificadores anonimizados y no anonimizados.

Como puede verse en la figura 3, un proveedor de datos referenciado como DS está conectado comunicativamente a través de una red pública o virtual privada a un agregador de datos referenciado como DA. La entidad proveedora de datos DS puede ser cualquier proveedor de movimiento y/o datos personales. Como se describe, DS y DA están físicamente separados y asignados a sistemas independientes. En general, DS y DA cumplen diferentes tareas que pueden asignarse a diferentes usuarios que tienen diferentes perfiles de autoridad en un sistema común o que se realizan dentro de diferentes zonas de seguridad de un sistema común.

Los ejemplos de realización de acuerdo con las figuras se basan en un sistema de red móvil como proveedor de datos DS que proporciona los conjuntos de datos mencionados anteriormente que contienen datos personales, así como datos de eventos de ubicación sobre sus abonados. Cada abonado individual de la red general del DS se identifica mediante un PID de identificador personal que podría ser un identificador conocido como el IMSI de un abonado. Para tener una anonimización real de acuerdo con las normas europeas de protección de datos, es necesario, entre otras cosas, separar el PID inicial y su contraparte, el O-PID (identificador personal ofuscado). En este contexto, el esfuerzo de reunir estos dos identificadores debe ser excesivamente alto en comparación con el rendimiento que podría obtenerse con tal acción. Este requisito se cumple si la separación se realiza físicamente dentro de las instalaciones de dos entidades legalmente independientes, por lo que una entidad solo conoce el PID y la otra solo el O-PID. Sin embargo, la separación de la DS y la DA también puede realizarse mediante una de las posibilidades alternativas tal como se propuso anteriormente. En cualquier caso, es necesario cifrar y transmitir el O-PID a un tercero nombrado como el agregador de datos DA. Ese identificador personal se combina en un conjunto de datos con atributos de datos adicionales que describen un determinado evento de ubicación. Por ejemplo, estos atributos de datos de eventos caracterizan una acción de un abonado en un lugar determinado. Los atributos posibles son el tipo de evento, la ubicación del evento y la marca de tiempo. En este ejemplo, el cifrado solo se realiza para el identificador personal, pero también se puede realizar para otros datos.

La ofuscación de los datos sensibles debe realizarse mediante un proceso de anonimización multinivel (MAP) realizado en el DS para proteger la privacidad del usuario. En la primera etapa 1, se realiza una anonimización básica aplicando un algoritmo de hashing con clave no reversible al PID, donde la clave (clave DS) solo la conoce el proveedor de datos DS. Dicho algoritmo de hash debe ser una función criptográfica de hash fuerte. Diferentes teclas DS pueden estar disponibles en el lado de DS con diferentes tiempos de vida como ST/LT (tiempo corto/tiempo largo), por ejemplo. La salida de la primera etapa del método es un solo PID ofuscado al que se hace referencia como O-PID. La vida útil de dicho O-PID depende del intervalo en el que se cambia la clave DS. Es decir, si la clave DS es, por ejemplo, constante durante 24 horas, el DA obtendrá un identificador ofuscado estático para ese período de tiempo exacto. El tipo de clave DS utilizada para ofuscar el PID depende de los atributos del conjunto de datos/datos que se transmiten al DA o a un tercero en combinación con el PID ofuscado. Por ejemplo, se utiliza una clave de corto plazo (clave ST) para ofuscar el PID que se envía en combinación con los datos de la clase del cliente en donde se usa una clave LT para el proceso MAP al ofuscar el PID para transmitir conjuntos de datos de eventos de ubicación.

En una segunda etapa 2, un componente o cadena aleatoria, por ej. preferiblemente, se agrega un número aleatorio de varios dígitos al O-PID de salida del procedimiento de anonimización base de acuerdo con la primera etapa 1. Se observa que el número aleatorio se puede insertar en cualquier posición del O-PID en el que el DA tiene que conocer la posición. Se señala además que cualquier otra cadena de caracteres generada aleatoriamente y cualquier otro procedimiento de combinación de las dos cadenas podrían ser apropiados. La longitud del intervalo del número aleatorio utilizado también podría ser variable, pero el DA debe conocerla. La salida de la segunda etapa se marca como O-PID+RC.

En la última etapa 3, un cifrado de segundo nivel que también se denomina cifrado adicional “AE” se ejecuta sobre la base de un mecanismo de cifrado asimétrico utilizando la clave pública DA-Pub-Key de la segunda entidad DA. El cifrado asimétrico se aplica al resultado de la etapa 2 O-PID+RC que resulta en un resultado que se marca como OO-PID. En consecuencia, el PID está ofuscado para proteger la privacidad del usuario.

La vida útil del identificador doble encriptado OO-PID solo depende del intervalo en el que se cambia el número aleatorio utilizado en la etapa 2. Esto significa que el OOPID es constante siempre que el RC sea constante, lo que es importante para los cálculos realizados en el OO-PID por un socio de confianza (por ejemplo, la construcción de índices estadísticos). En contraste, el valor real del número aleatorio no es necesario para la decodificación del OOPID en el DA.

Las etapas 1 a 3 se implementan en una unidad atómica de trabajo. Es imposible para el proveedor de datos DS leer o escribir cualquier información generada entre las etapas individuales.

El componente aleatorio utilizado en la etapa 2 puede cambiar en condiciones predeterminadas, preferiblemente para cada conjunto de datos.

Las etapas 2 y 3 se pueden realizar en múltiples iteraciones, cada iteración se realiza mediante una clave diferente.

En el lado del agregador de datos, el descifrado DA se ejecuta en el cifrado adicional de acuerdo con la etapa 3 utilizando su clave privada DA-Priv-Key para descifrar el identificador cifrado recibido OO-PID. El resultado O-PID+RC se procesará aún más borrando el número conocido de dígitos al final de la cadena que representa el número aleatorio. El producto resultante es el O-PID. La duración de este identificador cifrado único O-PID en el lado del agregador de datos DA se define por la longitud del intervalo de la clave DS generada. Si la longitud del intervalo de la clave DS ha transcurrido una nueva clave DS y, por lo tanto, se generará un nuevo O-PID en el DS.

El PID original solo es visible en el lado del proveedor de datos DS ya que el agregador de datos DA solo conoce el identificador cifrado único O-PID. Por lo tanto, es imposible crear un catálogo (una tabla que asigna cada PID no anonimizado a su contraparte anonimizada, el O-PID) dentro de las instalaciones de una sola parte.

El resultado del proceso de anonimización multinivel (MAP) explicado anteriormente es que el proveedor de datos DS no puede averiguar el PID ofuscado. Lo mismo se aplica al agregador de datos DA que no puede encontrar el PID original sobre la base del PID ofuscado suministrado.

Sin embargo, como se explica en la parte introductoria de la descripción, la desanonimización directa todavía es posible para los conjuntos de datos de eventos de ubicación que son activados por eventos visibles. Un atacante potencial podría observar un abonado y un evento visible y asignar su observación a un conjunto de datos de eventos de ubicación especificados suministrados por el proveedor de datos. En ese caso, se identifica al abonado anónimo, por ejemplo, el O-PID.

Para evitar la deanonimización directa, un componente adicional de anonimización que se refiere a la idea inventiva de la aplicación se integra en el proceso completo de anonimización. La figura 1 muestra una posible realización de la presente invención. Describe una solución técnica para la anonimización de diferentes conjuntos de datos entregados por un único proveedor de datos DS. La anonimización y la transmisión de estos conjuntos de datos a un único agregador de datos DA se procesa mediante procesos completamente separados que se ejecutan en el proveedor de datos DS. Los diferentes tipos de conjuntos de datos se pueden combinar en base a los identificadores iguales O-PID en el agregador de datos DA.

Todo el proceso se subdivide en dos procesos independientes de anonimización multinivel (MAP) donde los identificadores personales PID (como elementos únicos entre los conjuntos de datos) se anonimizan por separado y se transmiten al agregador de datos junto con sus respectivos conjuntos de datos. De este modo, el primer proceso 10 de MAP es responsable de transmitir los llamados datos de clase de cliente que incluyen atributos que clasifican a los abonados en diferentes grupos de clases de abonados, por ejemplo, grupos de género o edad.

El segundo proceso MAP 20 es responsable de transmitir los llamados conjuntos de datos de eventos de ubicación con atributos que incluyen el tipo de evento, una marca de tiempo cuando ocurrió el evento y la ubicación del abonado que define la ubicación donde ocurrió el evento. El conjunto de datos de ubicación incluye obligatoriamente al menos

una marca de tiempo, otros atributos como el tipo de evento y la ubicación son opcionales. El PID se anonimiza mediante la anonimización básica y el cifrado adicional que se realiza de forma iterativa dos veces.

Como puede verse en la figura 1, los conjuntos de datos de eventos de ubicación en combinación con su PID ofuscado se transmiten a un socio de confianza TP que ejecuta el filtrado 50 de datos de eventos de ubicación, que se refiere al método inventivo de la presente invención. Antes de la ejecución del proceso 50 de filtrado, se deshace el segundo cifrado 51 adicional. El proceso de filtrado de datos de eventos de ubicación de la invención solo aprobará los conjuntos de datos de eventos de ubicación que muestran un riesgo mínimo de desanonimización directa. Los conjuntos de datos de eventos de ubicación aprobados se transmitirán al agregador de datos DA. El agregador de datos puede utilizar los conjuntos de datos de eventos de ubicación aprobados para su posterior procesamiento.

Los detalles del proceso 50 de filtrado de datos de eventos de ubicación según la invención se explicarán sobre la base de las figuras 4a, 4b 4c que muestran varios diagramas de flujo de los subprocesos respectivos. La Figura 4a muestra un diagrama de bloques de las etapas necesarias para deshacer el cifrado adicional en el proceso 51 de la figura 1. En el bloque 100, el socio de confianza TP recibe un conjunto de datos de eventos de ubicación anónima. Debido al proceso anterior de anonimización de niveles múltiples (MAP) con k encriptaciones adicionales revertidas por el DA, cada conjunto de datos de eventos de ubicación no proporciona ninguna información al abonado individual al que se hace referencia al conjunto de datos de eventos de ubicación. Por ejemplo, en la figura 1k es igual a 2. Por lo tanto, en la segunda etapa 200, el último cifrado adicional del PID ofuscado se invierte utilizando la clave 210 privada. El producto 220 resultante es el PID ofuscado k-1 que incluye un componente aleatorio. El componente aleatorio se elimina en el bloque 230 dando como resultado un identificador anonimizado ofuscado k-1 en el bloque 240. Si solo se aplicó una iteración de cifrado adicional en el DS (k=1), el resultado será efectivamente el identificador anonimizado de base O-PID.

El conjunto 301 de datos de evento de ubicación que incluye el k-1-PID resultante de acuerdo con el bloque 240 y los atributos no cifrados se transfiere al proceso 50 de filtrado. El bloque de filtrado comienza con la llamada ofuscación de marca de tiempo de subproceso 300 que se muestra en la figura 4b. En el bloque 310, el subproceso verifica la base de datos/configuración de reglas 311 si existen reglas de filtrado especificadas según el tipo de evento del conjunto 301 de datos de eventos de ubicación. Por ejemplo, el bloque 310 verifica si el tipo de evento incluido del conjunto de datos del evento de ubicación es un evento observable, que puede ser observado por un atacante potencial. Si el tipo de evento es un tipo de evento no observable, el método pasará al bloque 340. Ejemplos de un tipo de evento observable son la transmisión de un mensaje corto, iniciar una llamada saliente, recibir una llamada entrante o iniciar una sesión de datos. Un ejemplo de un tipo de evento no observable es un procedimiento de traspaso dentro de una red de comunicación móvil que entrega un terminal móvil de un abonado desde una primera celda móvil a una celda móvil adyacente. Cabe señalar que este procedimiento de traspaso también se realiza durante el funcionamiento de una red de área de ubicación inalámbrica.

Si la parte confiable descubre que el tipo de evento del conjunto de datos de evento de ubicación comprobada es un tipo de evento observable, el método continúa con el bloque 330. En el bloque 330, el atributo de marca de tiempo incluido del conjunto de datos de evento de ubicación se confunde mediante manipulación. En detalle, la marca de tiempo se modificará como se describe a continuación para evitar cualquier desanonimización directa mediante la observación del evento respectivo. La modificación de la marca de tiempo se puede hacer asignando el evento a un marco de tiempo, redondeando la marca de tiempo real o compensando la marca de tiempo por cierto desplazamiento, preferiblemente determinado al azar. Luego, el método pasará al subproceso 400 para filtrar.

La Figura 4c divulga el filtrado de ubicaciones con muy poca actividad. En resumen, el proceso de filtrado compara la ubicación de varios conjuntos de datos de eventos de ubicación recibidos dentro de un cierto intervalo de tiempo de monitoreo y cuenta el número de diferentes PID confundidos para cada ubicación detectada. De este modo, se crea una lista de ubicaciones que cita todas las ubicaciones y la cantidad de OO-PID diferentes que activaron un evento en dicha ubicación. El intervalo de tiempo de monitoreo generalmente corresponde a la vida útil de la primera clave privada utilizada en el proveedor de datos para ofuscar el PID. El proceso de filtrado también se puede aplicar a los identificadores personales PID no confundidos como preprocesamiento de datos. En general, el proceso de filtrado de la invención es un proceso independiente que se puede realizar en cualquier etapa de la ubicación del sistema descrito o de cualquier otro sistema.

En detalle, en el bloque 401 se determina la ubicación del atributo de ubicación del conjunto de datos de eventos de ubicación recibidos y se compara con una lista 402 de ubicaciones. Si la lista ya contiene una ubicación coincidente, el ID anónimo (k-1)-PID se agrega a la ubicación almacenada en la etapa 404. Si la lista 402 no contiene una entrada coincidente, se crea una nueva ubicación como una nueva entrada en la lista 402 de ubicaciones y se marca como “bloqueada” de acuerdo con la etapa 403. Dichas ubicaciones que están marcadas como bloqueadas no están aprobadas para su transmisión a la entidad DA, en donde las ubicaciones marcadas como “desbloqueadas” están aprobadas para transmisión. Además, cada ubicación está marcada por su estado actual “bloqueado/desbloqueado” junto con una marca de tiempo que caracteriza el momento en el que se produjo un cambio de estado. Posteriormente la etapa 403, el (k-1)-PID se agregará a la nueva ubicación en la lista en la etapa 404.

En la siguiente etapa 405, el proceso verifica el estado actual de la ubicación a la que se ha agregado actualmente un (k-1)-PID. Si la ubicación está marcada como “desbloqueada”, el proceso volverá a verificar en la etapa 406 si el estado aún es elegible. Si la respuesta es “sí”, el conjunto de datos del evento de ubicación respectivo se reenvía a la siguiente etapa 500 de procesamiento, que incluye la transmisión al DA. Si la marca de la ubicación no es elegible, la ubicación se marca como “bloqueada” en la etapa 407 y el proceso continúa con la etapa 408, que también se ejecuta cuando la primera verificación en la etapa 405 revela que la ubicación actualmente está marcada como “bloqueada”.

La etapa 408 cuenta la cantidad de diferentes (k-1)-PID que se han agregado a la ubicación determinada del conjunto de datos de eventos de ubicación dentro de un cierto intervalo de tiempo. El comienzo de dicho intervalo se define por la marca de tiempo almacenada para cada ubicación. Si el número de k-1-PID diferentes por ubicación no excede un cierto umbral, el conjunto de datos de evento de ubicación respectivo se agrega a una cola 411 temporal en la etapa 409. Si el estado de estas ubicaciones permanece “bloqueado” durante un cierto intervalo de tiempo, se aplica un proceso de filtrado de eventos de ubicación a estos conjuntos de datos en el subproceso 600. El subproceso 600 se explicará más adelante.

Si el número supera el umbral, la ubicación se marca como “desbloqueada” junto con una marca de tiempo y todos los conjuntos de datos de eventos de ubicación incluidos en la cola 411 y en referencia a los PID contados (k-1) se reenvían a la siguiente etapa 500 de procesamiento, que es responsable de la transmisión de los conjuntos de datos al agregador de datos DA.

Los conjuntos de datos de eventos de ubicación que se refieren a ubicaciones “bloqueadas” que no se han desbloqueado en un determinado período de tiempo se pueden procesar mediante tres opciones diferentes en el subproceso 600.

Como primera opción, estos conjuntos de datos de eventos de ubicación se descartan por completo.

Como una segunda opción, es posible cancelar los (k-1)-PID incluidos en los conjuntos de datos de eventos de ubicación de las ubicaciones “bloqueadas”. Posteriormente, los conjuntos de datos de eventos de ubicación de ubicaciones “bloqueadas” se transmiten al agregador de datos sin ninguna información de identificación. De hecho, el agregador de datos DA puede usar los datos de eventos de ubicación recibidos para otras aplicaciones, sin embargo, no habrá referencia entre los diferentes conjuntos de datos de eventos de ubicación recibidos. Por ejemplo, no se puede determinar si uno o más abonados han generado diferentes conjuntos de datos.

Como una tercera opción, también es posible combinar los conjuntos de datos de eventos de ubicación de dos o más ubicaciones adyacentes y acumular su número de abonados diferentes. Por ejemplo, si la lista incluye dos ubicaciones que tienen cada una un número bajo de abonados diferentes, ambas ubicaciones se combinan entre sí para superar el umbral respectivo para el número de abonados diferentes.

Una ubicación puede definirse como un área geográfica determinada. Es preferible combinar las ubicaciones que muestran el número más bajo de abonados y ubicadas adyacentes entre sí. Si la combinación de ubicaciones no aprobadas no alcanza el umbral definido, también es posible combinar una ubicación no aprobada con una ubicación aprobada. Es obligatorio para la aprobación que las ubicaciones combinadas alcancen el umbral respectivo de los diferentes abonados. Si se supera el umbral necesario, los atributos de ubicación del conjunto de datos de evento de ubicación respectivo de ubicaciones combinadas se reemplazan por un atributo de ubicación común que define el área de ubicación combinada. Sin embargo, también es posible combinar áreas geográficas congéneres que no están ubicadas adyacentes entre sí. Posteriormente, dichos conjuntos de datos de eventos de ubicación se transmiten al agregador de datos DA.

La etapa de la combinación también se puede realizar aumentando el área geográfica y/o aumentando el radio de dicha área geográfica para la cual se cuenta el número de conjuntos de datos de eventos de ubicación y/o aumentando la imprecisión del área o la decisión de si un evento ocurrió dentro de dicha área

La Figura 2 muestra un enfoque ampliado de la realización representada en la Figura 1. Como puede verse, además del proceso de filtrado de datos de eventos de ubicación 50, el filtrado de datos de clase de cliente/datos estáticos se realiza en el TP de socio de confianza.

Los datos 10 de clase de cliente anonimizados se envían al TP de socio de confianza y se analizan mediante el proceso de filtrado de datos separados 60. De este modo, el proceso 60 de filtrado identifica perfiles demasiado específicos. Si se detecta dicho perfil, el proceso 60 de filtrado ofrece dos posibilidades diferentes.

Como primera opción, es posible eliminar todo el perfil detectado o, más bien, los conjuntos de datos de eventos de ubicación respectivos identificados por el proceso 60 de filtrado. Como segunda opción, es posible eliminar o generalizar solo los atributos individuales incluidos en los datos de la clase del cliente. Por ejemplo, si la fecha de la clase del cliente incluye atributos que se refieren a la edad o el sexo de un abonado determinado, es posible generalizar la edad del atributo. La generalización puede realizarse reemplazando la edad del atributo original, incluida una cierta edad por un intervalo de edad, por ejemplo, de 30 años a 40 años. Debido a esa manipulación de un determinado

atributo del grupo de clases de clientes, un determinado grupo de atributos contendrá más abonados diferentes. El número creciente de abonados por grupo complica la identificación de perfiles de abonados específicos. Por lo tanto, se evita una desanonimización indirecta a través de perfiles de datos estáticos individuales. Después de una generalización de los perfiles de datos estáticos, los datos del grupo de clientes se aprueban y se envían al agregador de datos DA.

REIVINDICACIONES

1. Un método para anonimizar los datos de eventos de ubicación recopilados dentro de una red de comunicaciones móviles que proporciona un servicio para los suscriptores o clientes en el que cada conjunto de datos de eventos de ubicación se relaciona con un suscriptor o cliente individual de la red de comunicaciones móviles especificada por un identificador personal confundido y consiste en de un atributo de evento que define un evento ocurrido de un suscriptor individual y de un atributo de ubicación que define la ubicación actual donde ocurrió el evento, caracterizado porque para cada ubicación detectada el método cuenta el número de diferentes identificadores personales confundidos que activan un evento en cada ubicación y en el que el método combina los conjuntos de datos de eventos de ubicación recopilados de diferentes ubicaciones, si el número de identificadores personales diferentes confusos en una ubicación es menor que un umbral definido.

2. El método de acuerdo con la reivindicación 1, en el que los atributos de ubicación de los conjuntos de datos de eventos de ubicación combinados se reemplazan por un atributo de ubicación generalizado.

3. El método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que se combinan conjuntos de datos de eventos de ubicación de al menos dos ubicaciones adyacentes.

4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que se combinan conjuntos de datos de eventos de ubicación con un número contado de diferentes identificadores personales confundidos por debajo del umbral definido.

5. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que los conjuntos de datos de eventos de ubicación de una ubicación con un número contado de diferentes identificadores personales confundidos por debajo del umbral definido se combinan con una ubicación con un número de conjuntos de datos de eventos de ubicación por encima del umbral definido.

6. El método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la generación y recopilación de un conjunto de datos de eventos de ubicación es activada por un suscriptor individual que solicita un determinado servicio de la red de comunicaciones móviles, por ejemplo, una transmisión de un mensaje corto, un mensaje entrante y/o una llamada telefónica saliente y/o una sesión de datos, un evento de traspaso o un evento de posicionamiento auto-iniciado del dispositivo terminal de abonado.

7. El método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que los conjuntos de datos de evento/ubicación de datos de evento incluyen un atributo de marca de tiempo que define el tiempo de evento en el que dicha marca de tiempo se modifica redondeando la marca de tiempo y/o agregando un desplazamiento de tiempo que es un conjunto ventajosamente aleatorio.

8. Un sistema de comunicación para realizar el método de acuerdo con cualquiera de las reivindicaciones 1 a 7.

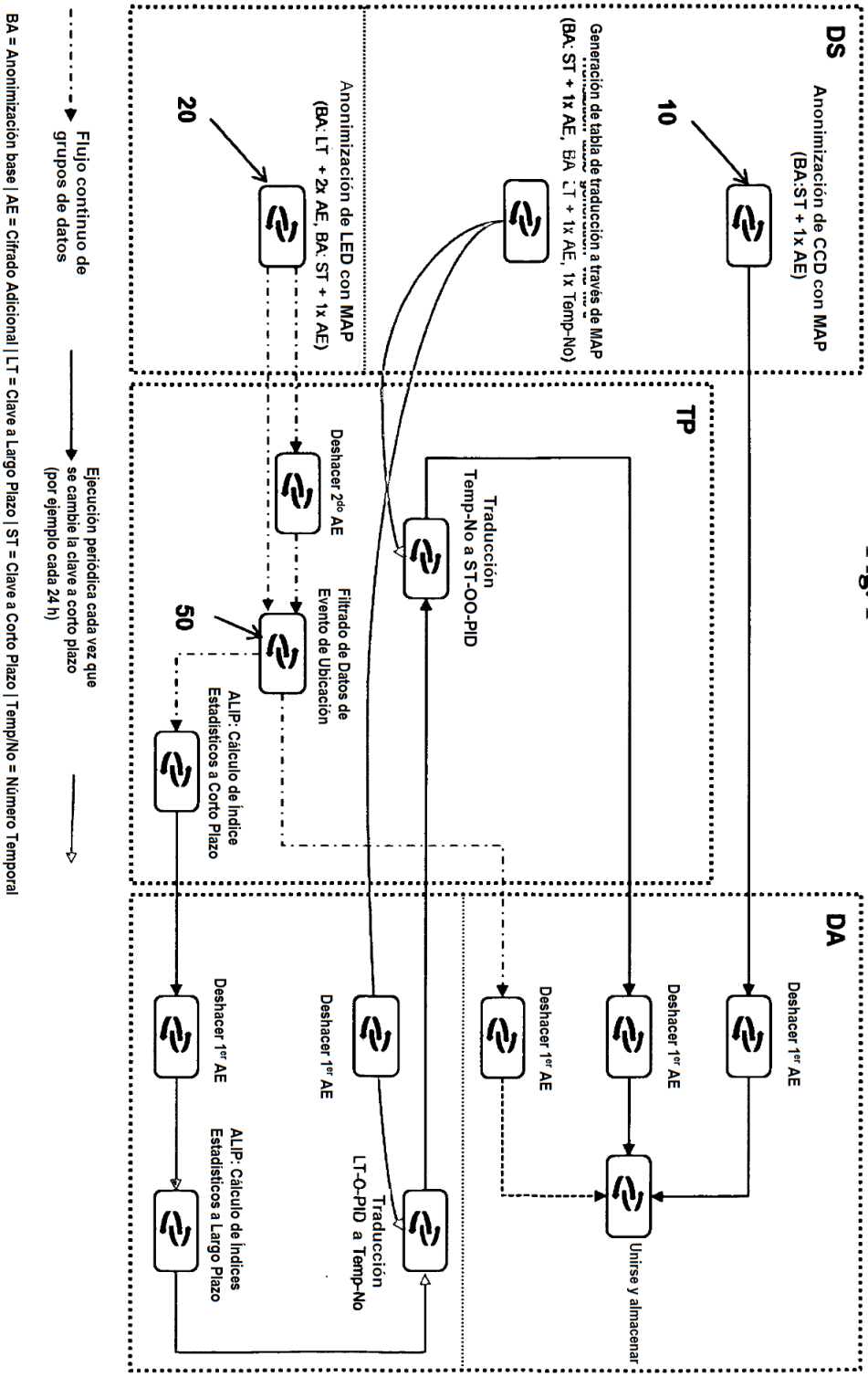

DS
Anonimización de CCD con MAP
(BA:ST + 1x AE)
10
Generación de tabla de traducción a través de MAP
(BA: ST + 1x AE, BA: LT + 1x AE, 1x Temp-No)
Anonimización de LED con MAP
(BA: LT + 2x AE, BA: ST + 1x AE)
20
TP
Traducción
Temp-No a ST-OO-PID
Deshacer 2do AE
Filtrado de Datos de
Evento de Ubicación
50
ALIP: Cálculo de Índice
Estadísticos a Corto Plazo
DA
Deshacer 1er AE
Deshacer 1er AE
Unirse y almacenar
Deshacer 1er AE
Deshacer 1er AE
Traducción
LT-O-PID a Temp-No
Deshacer 1er AE
ALIP: Cálculo de Índices
Estadísticos a Largo Plazo
Flujo continuo de
grupos de datos
Ejecución periódica cada vez que
se cambie la clave a corto plazo
(por ejemplo cada 24 h)
BA = Anonimización base | AE = Cifrado Adicional | LT = Clave a Largo Plazo | ST = Clave a Corto Plazo | Temp/No = Número Temporal

Fig. 1

Fig. 2

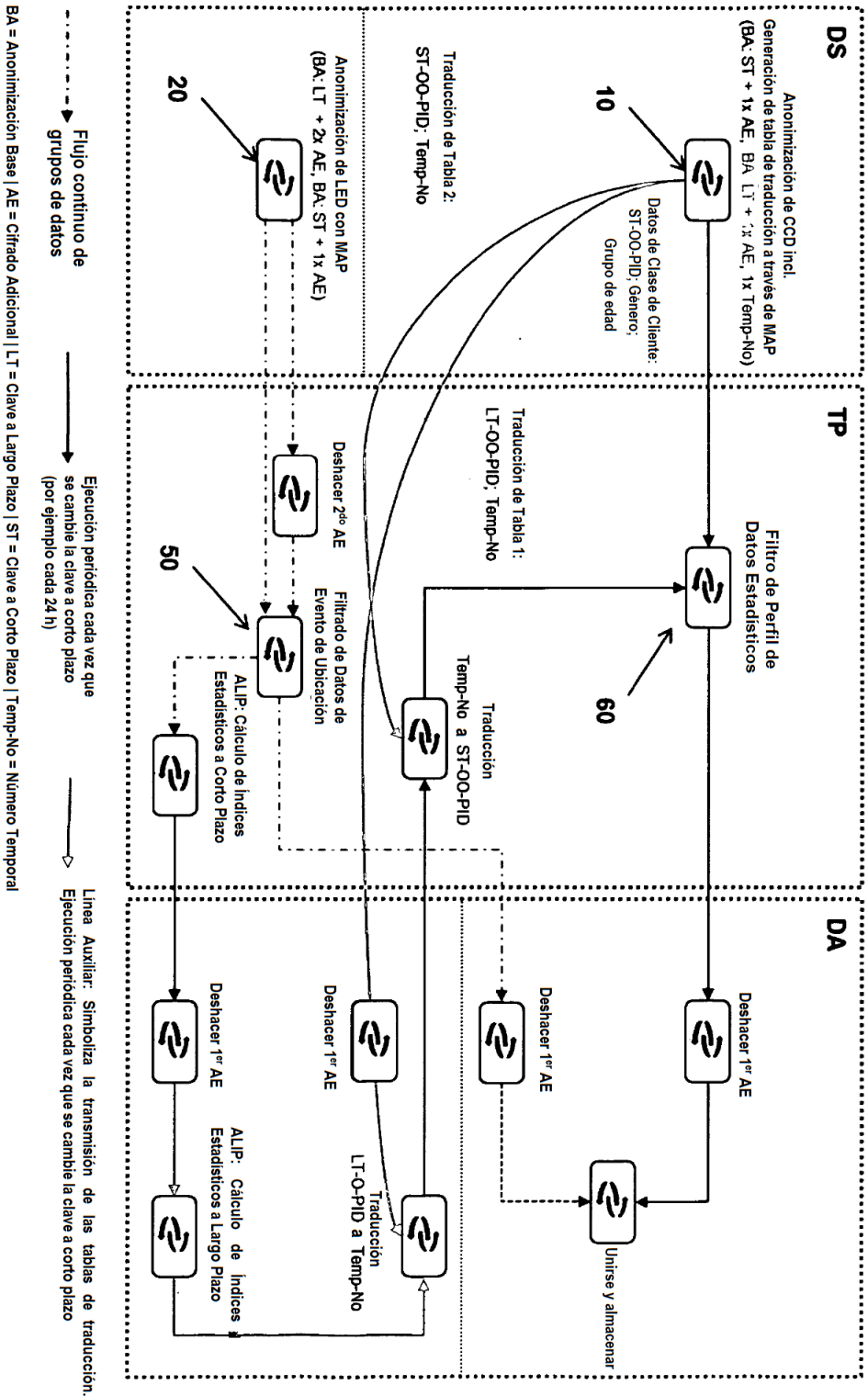

DS
TP
DA
Anonimización de CCD incl.
Generación de tabla de traducción a través de MAP
(BA: ST + 1x AE, BA: LT + 2x AE, 1x Temp-No)
10
Datos de Clase de Cliente:
ST-OO-PID; Genero;
Grupo de edad
Traducción de Tabla 2:
ST-OO-PID; Temp-No
Anonimización de LED con MAP
(BA: LT + 2x AE, BA: ST + 1x AE)
20
Filtro de Perfil de
Datos Estadísticos
60
Traducción de Tabla 1:
LT-OO-PID; Temp-No
Traducción
Temp-No a ST-OO-PID
Deshacer 2do AE
Filtrado de Datos de
Evento de Ubicación
50
ALIP: Cálculo de Índices
Estadísticos a Corto Plazo
Deshacer 1er AE
Unirse y almacenar
Deshacer 1er AE
Traducción
LT-O-PID a Temp-No
Deshacer 1er AE
ALIP: Cálculo de Índices
Estadísticos a Largo Plazo
Flujo continuo de
grupos de datos
Ejecución periódica cada vez que
se cambie la clave a corto plazo
(por ejemplo cada 24 h)
Linea Auxiliar: Simboliza la transmisión de las tablas de traducción.
Ejecución periódica cada vez que se cambie la clave a corto plazo
BA = Anonimización Base | AE = Cifrado Adicional | LT = Clave a Largo Plazo | ST = Clave a Corto Plazo | Temp-No = Número Temporal

Fig. 3

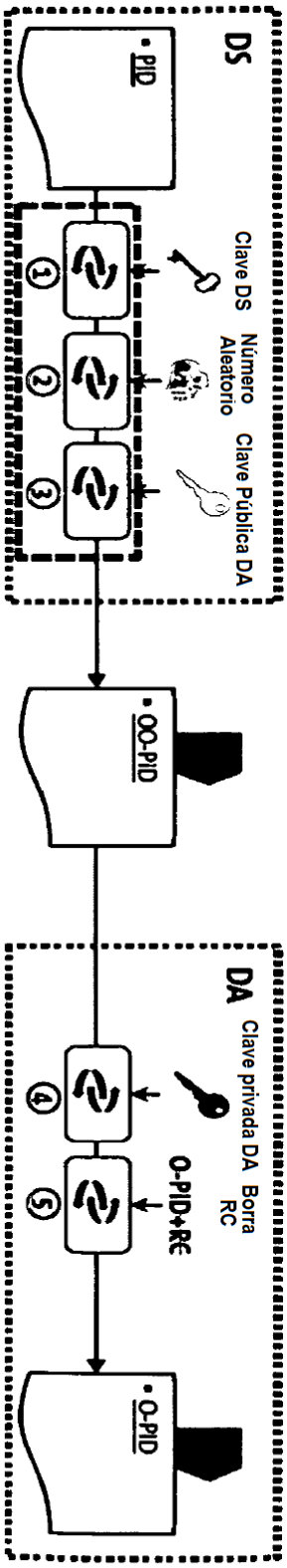

DS
PID
Clave DS
Número Aleatorio
Clave Pública DA
1
2
3
OO-PID
DA
Clave privada DA
Borra RC
O-PID+RE
4
5
O-PID

Fig. 4a

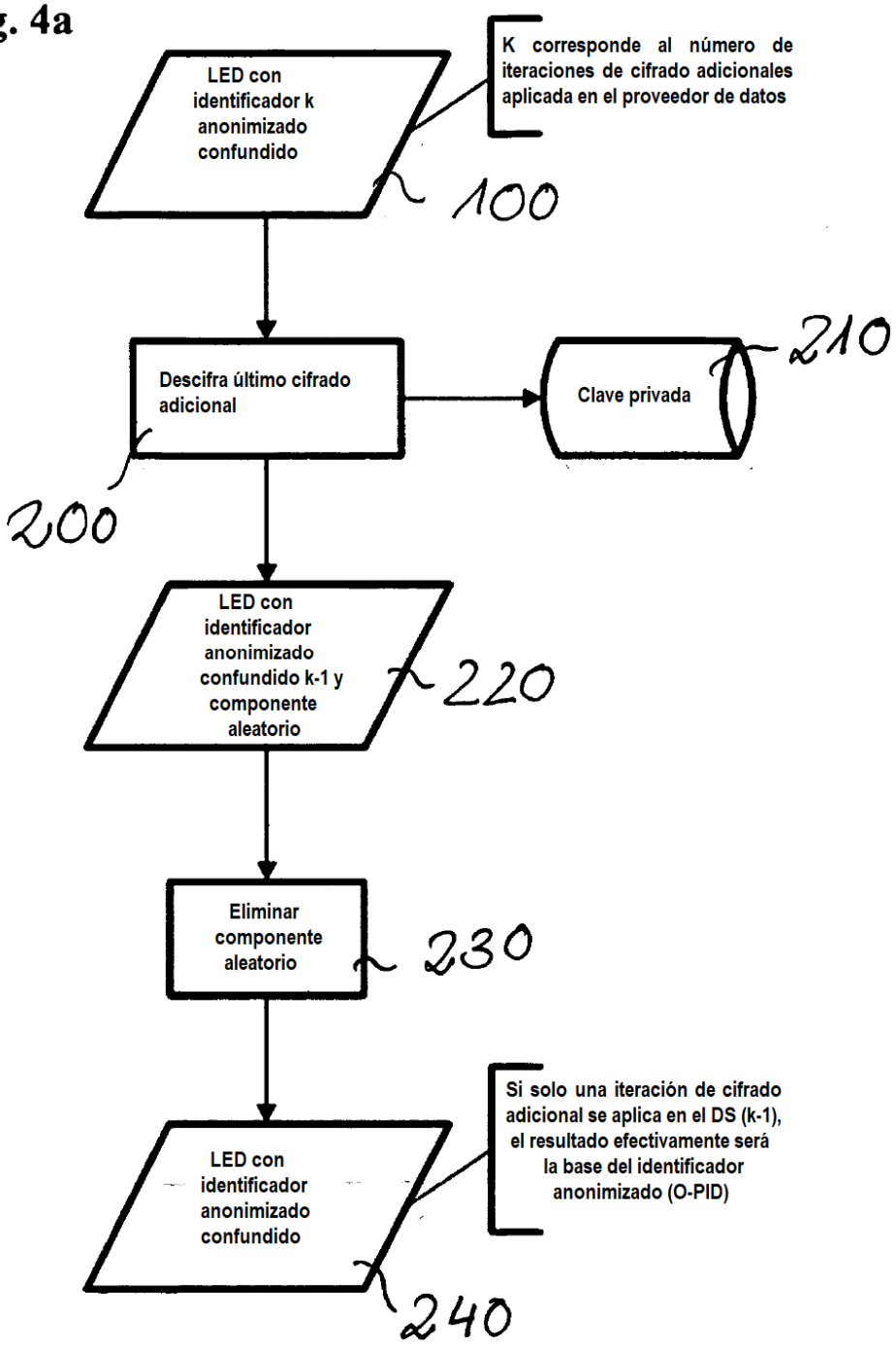

LED con identificador k anonimizado confundido
K corresponde al número de iteraciones de cifrado adicionales aplicada en el proveedor de datos
100
Descifra último cifrado adicional
Clave privada
210
200
LED con identificador anonimizado confundido k-1 y componente aleatorio
220
Eliminar componente aleatorio
230
LED con identificador anonimizado confundido
Si solo una iteración de cifrado adicional se aplica en el DS (k-1), el resultado efectivamente será la base del identificador anonimizado (O-PID)
240

Fig. 4b

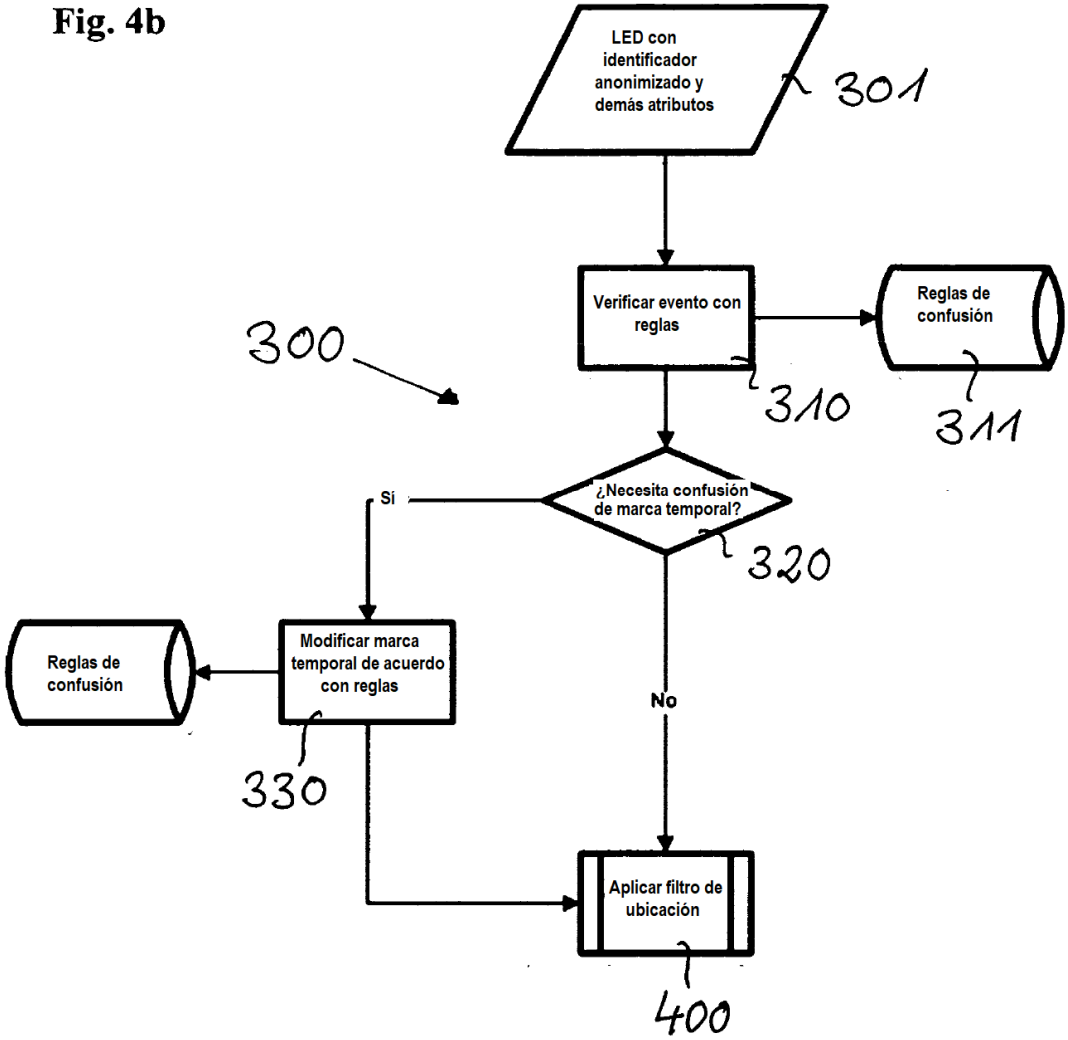
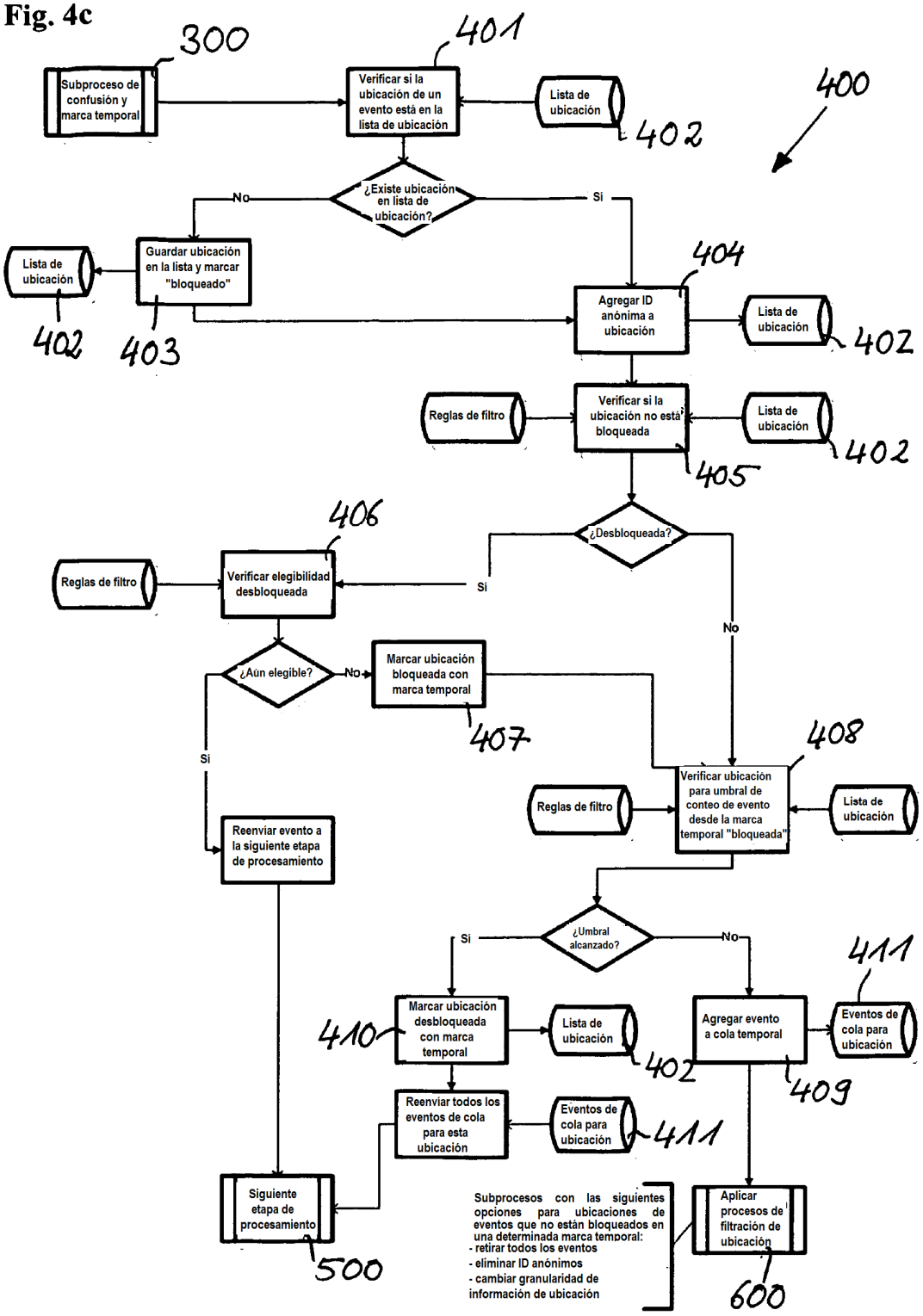

LED con identificador anonimizado y demás atributos
301
300
Verificar evento con reglas
310
Reglas de confusión
311
¿Necesita confusión de marca temporal?
320
Sí
No
Modificar marca temporal de acuerdo con reglas
330
Reglas de confusión
Aplicar filtro de ubicación
400

Fig. 4c


300
401
400
Subproceso de confusión y marca temporal
Verificar si la ubicación de un evento está en la lista de ubicación
Lista de ubicación
402
¿Existe ubicación en lista de ubicación?
No
Si
Guardar ubicación en la lista y marcar "bloqueado"
Lista de ubicación
403
404
Agregar ID anónima a ubicación
Lista de ubicación
Reglas de filtro
Verificar si la ubicación no está bloqueada
Lista de ubicación
405
¿Desbloqueada?
406
Reglas de filtro
Verificar elegibilidad desbloqueada
Si
No
¿Aún elegible?
No
Marcar ubicación bloqueada con marca temporal
407
Si
408
Reglas de filtro
Verificar ubicación para umbral de conteo de evento desde la marca temporal "bloqueada"
Lista de ubicación
Reenviar evento a la siguiente etapa de procesamiento
¿Umbral alcanzado?
Si
No
411
410
Marcar ubicación desbloqueada con marca temporal
Lista de ubicación
Agregar evento a cola temporal
Eventos de cola para ubicación
409
Reenviar todos los eventos de cola para esta ubicación
Eventos de cola para ubicación
Siguiente etapa de procesamiento
500
Subprocesos con las siguientes opciones para ubicaciones de eventos que no están bloqueados en una determinada marca temporal:
- retirar todos los eventos
- eliminar ID anónimos
- cambiar granularidad de información de ubicación
Aplicar procesos de filtración de ubicación
600