(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 504**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.01.2007 PCT/US2007/002497**

(87) Fecha y número de publicación internacional: **09.08.2007 WO07089758**

(96) Fecha de presentación y número de la solicitud europea: **29.01.2007 E 07762879 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.04.2017 EP 1980085**

(54) Título: **Procedimiento de autenticación segura de dispositivos móviles**

(30) Prioridad:

31.01.2006 US 343733

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.09.2017

(73) Titular/es:

ALCATEL-LUCENT USA INC. (100.0%)
600-700 Mountain Avenue
Murray Hill, NJ 07974, US

(72) Inventor/es:

BROK, JACCO;
ZIVKOVIC, MIROSLAV;
LAGERBERG, KO y
TEUNISSEN, HAROLD

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de autenticación segura de dispositivos móviles

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere, en general, a sistemas de comunicación y, más en particular, se refiere a sistemas de comunicación inalámbrica.

2. Descripción de la técnica relacionada

Los sistemas de comunicación inalámbrica se emplean comúnmente para proporcionar comunicaciones de voz y / o datos. Los sistemas de comunicación inalámbrica existentes y emergentes generalmente están compuestos por colecciones heterogéneas de tecnologías de interfaz de aire, arquitecturas de red y protocolos inalámbricos. Por ejemplo, los sistemas de comunicación inalámbrica pueden operar utilizando redes inalámbricas IEEE - 802.11 (Wi - Fi) que proporcionan acceso a redes de área local y a puntos de acceso inalámbrico, conectividad Bluetooth, redes IEEE - 802.16 (WiMax) que proporcionan acceso fijo inalámbrico y banda ancha móvil, redes de Datos de Evolución Optimizados (IxEVDO) que proporcionan acceso a usuarios de datos móviles de tercera generación (3G), y otros similares.

Las comunicaciones inalámbricas introducen un nuevo grado de riesgo de seguridad con respecto a los sistemas terrestres convencionales. En un entorno inalámbrico, los adversarios son capaces de escuchar con más facilidad las comunicaciones puesto que la información se envía a través de un enlace inalámbrico que se considera que es más accesible que los canales terrestres convencionales. Además, con la proliferación de dispositivos móviles (por ejemplo, ordenadores portátiles, teléfonos celulares, asistentes personales digitales y otros similares), los usuarios son cada vez más susceptibles a ataques adversarios que intentan obtener acceso no autorizado a datos almacenados.

En entornos públicos, por ejemplo, tales como un terminal de aeropuerto, los adversarios pueden intentar escuchar a escondidas las comunicaciones inalámbricos para interceptar datos de autenticación, tales como contraseñas, direcciones de control de acceso a medios (MAC), números de identificación personal (PIN), claves de seguridad y otros similares. Los adversarios pueden usar esta información para obtener acceso no autorizado a sistemas de comunicación inalámbrica y / o a otros dispositivos móviles. Para ilustrar este punto, en el caso del protocolo Bluetooth, un adversario puede escuchar a escondidas durante el emparejamiento de los dispositivos móviles. Tal como se utilizan en la presente memoria descriptiva, los términos "autenticación", "autenticar", "emparejamiento" y "par" están destinados a ser utilizados indistintamente para referirse en general a algoritmos, procesos, mecanismos y / o datos utilizados para establecer comunicaciones confiables. Durante el proceso de emparejamiento, el adversario puede "escuchar" para interceptar los PIN de uno o más dispositivos móviles. Con esta información, el adversario puede decodificar datos necesarios para emparejarse con uno o más de los dispositivos móviles que participan en la comunicación inalámbrica. Si tiene éxito, el adversario puede obtener acceso no autorizado a datos personales, tales como datos de calendario, libretas de direcciones, correo electrónico, información de tarjetas de crédito y otros similares.

Un algoritmo de ataque de ejemplo se describe, por ejemplo, en un artículo titulado "Desciframiento de PIN de Bluetooth" de Yaniv Shaked y Avishai Wool. En este artículo, con respecto al protocolo Bluetooth, los autores describen un defecto que existe en basarse únicamente en un PIN de n dígitos para emparejar un dispositivo móvil con otro. En particular, los autores describen un algoritmo que se puede usar con un PIN interceptado de un dispositivo móvil para "descifrar" los mecanismos convencionales de autenticación de Bluetooth en menos de un segundo. Otros protocolos utilizados en diferentes tecnologías inalámbricos, tales como Wi - Fi, IxEVDO y otros similares, sufren de deficiencias similares y los adversarios han probado la interceptación con éxito de datos de autenticación y el uso de estos datos para obtener acceso no autorizado a datos confidenciales. El documento US 2003/0200434A1 muestra un procedimiento de identificación seguro entre dos aparatos de RF en el que los aparatos se mueven para acercarse uno al otro para el emparejamiento.Lo que se necesita, por lo tanto, es un mecanismo de autenticación que, cuando se solicite, garantice mejor que sólo los dispositivos móviles de confianza se permitan emparejarse unos con los otros y / o intercambiar datos con una red de comunicación inalámbrica.

La presente invención está dirigida a abordar los efectos de uno o más de los problemas que se han expuesto más arriba.

Sumario de la invención

La invención proporciona un procedimiento para autenticar un dispositivo móvil, un sistema y dispositivo móvil respectivos como se reivindica en las reivindicaciones independientes. Las realizaciones son reivindicadas en las reivindicaciones dependientes.Lo que sigue presenta un sumario simplificado de la invención con el fin de proporcionar una comprensión básica de algunos aspectos de la invención. Este sumario no es un resumen exhaustivo de la invención. No pretende identificar elementos clave o críticos de la invención o delinear el alcance de la invención. Su único propósito es presentar algunos conceptos en una forma simplificada como un preludio a la descripción más detallada que se explicará más adelante.

En un aspecto de la presente invención, se proporciona un procedimiento de autenticación de un dispositivo móvil. El procedimiento incluye recibir una solicitud de comunicación desde el dispositivo móvil. El dispositivo móvil es operativo para intercambiar datos a través de un canal primario. Los datos de autenticación son recibidos desde el dispositivo móvil a través de un canal secundario. El canal secundario es un canal de corto alcance operativo para intercambiar datos cuando el dispositivo móvil está dentro de una proximidad física. Los datos de autenticación se procesan para determinar si el dispositivo móvil es un dispositivo de confianza. En otro aspecto de la presente invención, se proporciona un procedimiento de autenticación de un dispositivo móvil.

El procedimiento incluye transmitir una solicitud de comunicación desde el dispositivo móvil. El dispositivo móvil es operativo para intercambiar datos a través de un canal primario. Los datos de autenticación se transmiten desde el dispositivo móvil a través de un canal secundario. El canal secundario es un canal de corto alcance operativo para intercambiar datos con una parte receptora cuando el dispositivo móvil y la parte receptora están dentro de una proximidad física. La parte receptora procesa los datos de autenticación para determinar si el dispositivo móvil es un dispositivo de confianza.

Breve descripción de los dibujos

La invención se puede entender haciendo referencia a la descripción que sigue tomada en conjunto con los dibujos que se acompañan, en el que los mismos números de referencia identifican elementos similares y en el que: la figura 1 es un diagrama de bloques simplificado de una red de comunicación inalámbrica ilustrativa;

La figura 2 es un diagrama de bloques simplificado que ilustra la comunicación inalámbrica de móvil a móvil entre uno o más dispositivos móviles;

La figura 3 ilustra conceptualmente una realización ejemplar de un procedimiento de autenticación de un dispositivo móvil de acuerdo con una realización de la presente invención; la figura 4 es un diagrama de bloques simplificado que ilustra el procedimiento de autenticación que se muestra en la figura 3 de acuerdo con una realización de la presente invención; y

La figura 5 es un diagrama simplificado de un dispositivo móvil que ilustra un mecanismo de autenticación de acuerdo con una realización de la presente invención.

Descripción detallada de realizaciones especificas

A continuación se describen realizaciones ilustrativas de la invención. En aras de la claridad, no todas las características de una implementación real se describen en esta memoria descriptiva. Por supuesto, se apreciará que en el desarrollo de cualquier realización real de este tipo, se deben tomar numerosas decisiones específicas de implementación para alcanzar los objetivos específicos de los desarrolladores, tales como el cumplimiento de las limitaciones relacionadas con el sistema y las relacionadas con el negocio, que variarán de una implementación a otra. Además, se apreciará que un esfuerzo de desarrollo de este tipo puede ser complejo y lento, pero sin embargo será una tarea rutinaria para los expertos en la técnica que tengan el beneficio de esta revelación.

Porciones de la presente invención y la descripción detallada correspondiente se presentan en términos de software, o algoritmos y representaciones simbólicas de operaciones de bits de datos dentro de una memoria de ordenador. Estas descripciones y representaciones son aquellas con las que los expertos en la técnica transmiten efectivamente la sustancia de su trabajo a otros expertos en la técnica. Un algoritmo, como se utiliza el término en la presente memoria descriptiva, y como se utiliza en general, se concibe como una secuencia auto - consistente de pasos que conducen a un resultado deseado. Los pasos son aquellos que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades toman la forma de señales ópticas, eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas y manipuladas de otra manera. Se ha probado conveniente a veces, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números u otros similares.

Se debe tener en cuenta, sin embargo, que todos estos términos y similares deben asociarse con las cantidades físicas apropiadas y son etiquetas meramente convenientes aplicadas a estas cantidades. A menos que se establezca específicamente lo contrario, o como es evidente de la explicación, términos tales como "procesamiento" o "computación" o "cálculo" o "determinación" o "visualización" u otros similares, se refieren a la acción y procesos de un sistema de ordenador, o dispositivo informático electrónico similar, que manipula y transforma datos representa-

dos como cantidades físicas, electrónicas dentro de los registros y memorias del sistema informático en otros datos representados de manera similar como cantidades físicas dentro de las memorias o registros del sistema informático u otros dispositivos de almacenamiento, transmisión o visualización de información de este tipo.

Se hace notar también que los aspectos implementados por software de la invención se codifican típicamente en alguna forma de medio de almacenamiento de programas o se implementan a través de algún tipo de medio de transmisión. El medio de almacenamiento de programas puede ser magnético (por ejemplo, un disquete o un disco duro), óptico (por ejemplo, un disco compacto de sólo lectura o "CD ROM") o basado en otras tecnologías y puede ser de sólo lectura o de acceso aleatorio. De forma similar, el medio de transmisión puede ser pares de alambres trenzados, cable coaxial, fibra óptica, transmisión inalámbrica, o algún otro medio de transmisión adecuado conocido en la técnica. La invención no está limitada por estos aspectos de ninguna implementación dada.

La presente invención se describirá a continuación con referencia a las figuras adjuntas. En los dibujos se ilustran esquemáticamente diversas estructuras, sistemas y dispositivos con fines de explicación solamente y con el fin de no oscurecer la presente invención con detalles que son bien conocidos por los expertos en la técnica. Sin embargo, los dibujos adjuntos se incluyen para describir y explicar ejemplos ilustrativos de la presente invención. Las palabras y frases utilizadas en la presente memoria descriptiva se deben entender e interpretar como que tienen un significado coherente con la comprensión de esas palabras y frases por los expertos en la técnica relevante. Ninguna definición especial de un término o frase, por ejemplo, una definición que sea diferente del significado ordinario y habitual tal como se entiende por los expertos en la técnica, se pretende que esté implícita por el uso consistente del término o frase en la presente memoria descriptiva. En la medida en que se pretende que un término o frase tenga un significado especial, es decir, un significado distinto del entendido por los expertos en la técnica, tal definición especial será expresamente expuesta en la memoria descriptiva de una manera de definición que proporcione directa e inequívocamente la definición especial para el término o frase.

Volviendo a continuación a los dibujos, y haciendo referencia específicamente a la figura 1, se ilustra una red de comunicaciones inalámbricas 100. Los términos "red de comunicación inalámbrica", "red móvil" y "red inalámbrica" se usan indistintamente en la presente memoria descriptiva para describir de manera general una red de comunicaciones que es operativa para proporcionar comunicación móvil a sus abonados. Por ejemplo, la red de comunicaciones inalámbricas 100 puede ser una red IxEVDO que por lo general cumple con las especificaciones técnicas y los informes técnicos de un Sistema Móvil de 3ª Generación que ha sido desarrollado por un Proyecto de Cooperación de 3ª Generación (3GPP).Se debe entender, sin embargo, que la presente invención puede ser aplicable a las redes de comunicación inalámbrica que soportan otros protocolos inalámbricos, tales como Wi - Fi, Bluetooth, WiMax y otros similares.

La red de comunicación inalámbrica 100 permite que uno o más dispositivos móviles 105 comuniquen con una red de datos 110, tal como Internet, y / o una Red Telefónica Pública con Conmutación (PSTN) 115 a través de uno o más puntos de acceso 120 (por ejemplo, estaciones base, transceptores Wi - Fi, etc.). Los dispositivos móviles 105 pueden adoptar la forma de cualquiera de una variedad de dispositivos, incluyendo teléfonos celulares, asistentes digitales personales (PDA), ordenadores portátiles, buscapersonas digitales, tarjetas inalámbricas y cualquier otro dispositivo electrónico de tipo similar. En una realización, una pluralidad de puntos de acceso 120 pueden estar acoplados a una red central (CN) 125 por una o más conexiones 130, tales como líneas o circuitos T1 / EI, circuitos ATM, cables, líneas de abonado digital (DSL) y otros similares. Además, la red de comunicaciones 100 puede estar compuesta por otros dispositivos (no mostrados), tales como controladores de red de radio (RNC), procesadores de gestión, y otros similares.

En general, la CN 125 funciona como una interfaz con una red de datos 110 y / o con la PSTN 115. La CN 125 puede realizar una variedad de funciones y operaciones, tales como autenticación de usuarios. Sin embargo, como se describirá más detalladamente a continuación, el proceso de autenticación de un dispositivo móvil 105 para comunicación de confianza puede ser realizado por cualquier número de dispositivos en la red de comunicaciones 100, tal como el punto de acceso 120 u otros dispositivos (no mostrados). Además, para las comunicaciones de móvil a móvil (por ejemplo, maestro / esclavo, entre iguales, etc.), el procesamiento de autenticación puede ser realizado por uno o más dispositivos móviles 105. Por lo tanto, se apreciará que una descripción detallada de la estructura y funcionamiento de la CN 125 no es necesaria para una comprensión y apreciación de la presente invención. Por consiguiente, para evitar ofuscar innecesariamente la presente invención, no se presentan en la presente memoria descriptiva más detalles de la CN 125.

Los expertos en la técnica apreciarán que la red de comunicación inalámbrica 100 facilita las comunicaciones entre los dispositivos móviles 105, la red de datos 110 y / o la PSTN 115. Se debe entender, sin embargo, que la configuración de la red de comunicación inalámbrica 100 es de naturaleza ejemplar y que se pueden emplear menos o más componentes adicionales en otras realizaciones del sistema de comunicaciones 100 sin apartarse del espíritu y el alcance de la presente invención.

La figura 2 ilustra la comunicación de móvil a móvil entre una pluralidad de dispositivos móviles 105. Aunque sólo se ilustran tres dispositivos móviles 105 para este ejemplo particular, se debe apreciar que la comunicación de móvil a

móvil es posible entre dos o más dispositivos móviles 105. Además, aunque no se muestra, uno o más de los dispositivos móviles 105 puede estar también en comunicación de datos con una red de comunicación, tal como la red de comunicaciones 100 que se ilustra en la figura 1. Cuando uno o más dispositivos móviles 105 están en comunicación de datos con una red de comunicación, se debe apreciar que bajo ciertas configuraciones otros dispositivos móviles 105 se pueden comunicar (por ejemplo, intercambiar datos) con la red de comunicación, a través de la comunicación de móvil a móvil.

La comunicación de móvil a móvil se puede implementar utilizando cualquier número de tecnologías y protocolos inalámbricos conocidos o que vayan a ser desarrollados. En la figura 2, se muestran los dispositivos móviles 105 que se comunican a través de un canal primario 200. El canal primario 200 es típicamente un canal de radiofrecuencia, pero también se pueden usar otras tecnologías inalámbricas tales como infrarrojos, ópticas y similares. De forma similar, el canal primario 200 se puede configurar para adaptarse a cualquier número de protocolos conocidos o que vayan a ser desarrollados, tales como IEEE 802.3 (Ethernet), acceso múltiple por división de código (CDMA), Bluetooth, sistema global para comunicaciones móviles (GSM), y otros similares.

Haciendo referencia a la figura 3, se muestra un procedimiento ilustrativo para autenticar un dispositivo móvil 105 de acuerdo con la presente invención. Para facilitar la descripción, el procedimiento se describe con referencia a la red de comunicación 100 y la comunicación de móvil a móvil que se muestra en las figuras 1 y 1, respectivamente. Se debe apreciar, sin embargo, que el procedimiento es igualmente aplicable a otras redes inalámbricas y configuraciones de móvil a móvil.

En el bloque 300, se recibe una solicitud de comunicación desde un dispositivo móvil 105. Como se ha descrito, el dispositivo móvil 105 se puede operar para que comunique a través de un canal primario 200. El canal primario 200 es el canal de comunicación de datos deseado para una tecnología inalámbrico dada y, típicamente proporciona al dispositivo móvil 105 cierta libertad de movimiento, manteniendo al mismo tiempo la comunicación de datos. En una red Wi - Fi, por ejemplo, el canal primario es habitualmente un canal de radiofrecuencia entre el dispositivo móvil 105, un punto de acceso 120 y / u otro dispositivo móvil 105. Para comunicaciones Bluetooth, el canal primario 200 se realiza típicamente entre dos o más dispositivos móviles 105. Sin embargo, el canal primario 200 también puede incluir comunicación con otros dispositivos, tales como ordenadores de sobremesa, quioscos electrónicos, o cualquier otro dispositivo electrónico capaz de interpretar la solicitud de comunicación.

Haciendo referencia a la figura 4, se muestra un canal primario 400 para la comunicación de datos entre un primer dispositivo 405 y un segundo dispositivo 410. En una realización, tanto los dispositivo primero como segundo 405, 410 son dispositivos móviles, y el canal primario 400 es un canal de comunicación de móvil a móvil. En otra realización ilustrativa, sólo uno de los dispositivos 405, 410 es un dispositivo móvil y el otro es un punto de acceso a una red de comunicación. Generalmente, los dispositivos primero y segundo 405 y 410 pueden ser cualquier dispositivo electrónico capaz de comunicación inalámbrica. Además, se debe apreciar que otros dispositivos electrónicos adicionales (no mostrados) también pueden ser capaces de comunicarse con los dispositivos primero y segundo 405, 410 usando el canal primario 400.

Como se describirá a continuación, para establecer una comunicación fiable entre los dos dispositivos 405, 410 (es decir, emparejar los dispositivos 405, 410) y / u otros dispositivos (no mostrados), un canal secundario 415 que es operativo para comunicaciones de corto alcance se utiliza para intercambiar datos de autenticación. Para simplificar la ilustración del proceso de autenticación, los ejemplos se centrarán principalmente en el caso en el que el canal secundario 415 se utilice para emparejar dos o más dispositivos móviles. Sin embargo, como ya se ha descrito, la invención no está limitada a esta manera, y se debe apreciar que el canal secundario 415 se puede realizar entre un dispositivo móvil 105 y un dispositivo fijo y / o cualquier número de otras configuraciones inalámbricas.

En el ejemplo ilustrativo que se muestra en la figura 4, el segundo dispositivo 410 recibe una solicitud de comunicación del primer dispositivo 405. Por ejemplo, la solicitud de comunicación puede ser una señal del primer dispositivo 405 que indica una intención de emparejarse con el segundo dispositivo 410. La solicitud de comunicación es normalmente generada por un dispositivo que desea iniciar una comunicación inalámbrica. Se debe entender que la solicitud de comunicación puede ser generada por cualquier dispositivo para indicar un deseo de participar en la comunicación inalámbrica.

La forma de la solicitud de comunicación puede variar dependiendo de la tecnología inalámbrica. Ordinariamente, la solicitud incluye datos que el receptor reconocerá e interpretará como una solicitud de comunicación. Además, la solicitud de comunicación se transmite a través del canal primario 400.

Como se ha descrito, el canal secundario 415 es un canal de corto alcance que utiliza la proximidad física para intercambiar datos, mientras que, con respecto al canal secundario 415, el canal primario 400 es un canal de mayor alcance que permite una mayor movilidad física.Con referencia de nuevo a la figura 3, en el bloque 305, se reciben datos de autenticación desde el dispositivo móvil 105 por el canal secundario 415. Como se ha descrito, el canal secundario 415 es un canal de corto alcance que depende de la proximidad física para intercambiar datos. A diferencia del canal primario 400 que permite una mayor distancia de separación, el canal secundario 415 requiere que

el dispositivo móvil sea colocado próximo al dispositivo con el que está intentando autenticarse. Esta proximidad física hace que sea más difícil, si no imposible, que un adversario se empareje con otra parte sin ser detectado. Esto es debido a que, durante el proceso de emparejamiento, el adversario ya no puede confiar en el canal primario 400 para mantener una distancia segura de su objetivo.

En una realización ilustrativa, el canal secundario 415 se realiza utilizando tecnología de identificación por radiofrecuencia (RFID). Una ventaja de la RFID es que no requiere un contacto directo o un barrido de línea de vista, pero sí se basa en la ventaja de la proximidad física que se ha descrito para el canal secundario 415. Haciendo referencia a la figura 4, en el caso ilustrativo de la RFID, el primer dispositivo 405 puede estar equipado con una etiqueta de RFID (no mostrada). En este ejemplo, la etiqueta de RFED puede ser parte de un controlador de autenticación 420. Se debe apreciar, sin embargo, que el controlador de autenticación 420 y otros componentes que se muestran para el primer y segundo dispositivos 405 y 410 están destinados a fines ilustrativos y no limitativos. Los expertos en la técnica apreciarán que la funcionalidad que se ha descrito en la presente memoria descriptiva puede ser configurada para ser operativa con menos o más que los componentes que se muestran en las figuras adjuntas y que la configuración real del sistema puede variar como un asunto de elección del diseño.

La etiqueta de RFID puede ser activa o pasiva. Una etiqueta de RFID activa está asociada típicamente a su propia fuente de alimentación, mientras que las etiquetas pasivas son etiquetas de RFID sin una fuente de alimentación. Las etiquetas pasivas normalmente se activan temporalmente mediante la exploración de la radiofrecuencia de un lector. Sin embargo, la configuración y el funcionamiento particulares de las etiquetas de RFID activas y pasivas pueden variar dependiendo de la aplicación particular.

En la figura 4, el primer dispositivo 405 está equipado con un transmisor 425, tal como una antena, para transmitir datos asociados a la etiqueta de RFID a otro dispositivo. Cuando se activa, la etiqueta de RFID normalmente genera una señal que incluye datos de identificación tales como un número de identificación. En este ejemplo ilustrativo, el segundo dispositivo 410 está configurado con un lector 430 para recibir los datos asociados con la etiqueta de RFID del primer dispositivo 405.

La distancia de trabajo de la RFID suele ser mucho menor que las tecnologías inalámbricas típicas, como Bluetooth, Wi - Fi y similares. Con la RFID pasiva, por ejemplo, el canal secundario 415 usado para transmitir datos de RFID (es decir, datos de autenticación) es típicamente de aproximadamente 1 metro o menor. En el caso de Bluetooth, el canal primario es ordinariamente de alrededor de 10 metros. En consecuencia, la RFID impone la proximidad física deseada para reducir o posiblemente eliminar el emparejamiento no autorizado. En la práctica, por ejemplo, se requeriría a un usuario con un dispositivo móvil 105 equipado con una etiqueta de RFID mantener físicamente su dispositivo móvil 105 aproximadamente 50 cm o más cerca de la otra parte para leer / intercambiar datos de RFBD. Sería difícil, si no imposible, que un adversario llegara a una proximidad física tan estrecha y evitase la detección. En otro ejemplo ilustrativo, ambas partes 405 y 410 están configuradas con etiquetas de RFID, transmisores 425 y lectores 430. En este ejemplo, ambas partes 405, 410 y cualquier otra parte que desee emparejarse pueden intercambiar datos de RFID para determinar si las partes son de confianza.

Haciendo referencia de nuevo a la figura 3, en el bloque 310, los datos de autenticación recibidos se procesan para determinar si el dispositivo móvil 105 es un dispositivo de confianza (es decir, determinar si es un dispositivo autorizado que está intentando emparejarse). En el ejemplo de la RFID anterior, la etiqueta de RFID genera los datos de autenticación, que tal como se describe pueden incluir datos de identificación. Los datos de identificación pueden incluir cualquier cadena binaria de datos operativo para identificar de forma única el dispositivo móvil 105. El segundo dispositivo 410 lee los datos de autenticación y los pasa al controlador de autenticación 420.

El controlador de autenticación 420 se puede configurar para determinar si es un dispositivo de confianza que intenta emparejarse. En un ejemplo ilustrativo, los datos de autenticación se pueden usar como entrada de parámetros en un algoritmo de autenticación programado en el controlador de autenticación 420. En otras palabras, la información de la RFID se puede usar como una semilla para el proceso de emparejamiento. Después de procesar la información de la RFID a través de su algoritmo de autenticación programado, el controlador de autenticación 420 puede determinar si un resultado esperado es retornado. Si es así, el controlador de autenticación 420 determina que se está comunicando con un dispositivo de confianza y permite que el proceso de emparejamiento se complete.

Se debe apreciar que la complejidad del algoritmo de autenticación usado para procesar los datos de autenticación (por ejemplo, información de la RFID) se puede variar como una cuestión de elección de diseño. En un caso simple, el controlador de autenticación 420 puede comparar los datos de autenticación con los valores almacenados para determinar si existe una coincidencia. Si es así, el dispositivo emisor se considera un dispositivo de confianza. En un caso complejo, los datos de autenticación intercambiados a través del canal secundario 415 se pueden configurar para variar en ciertos intervalos, de tal manera que sirva una sola vez (es decir, un parámetro variable en el tiempo) para el algoritmo de autenticación. Por ejemplo, la información de la RFID se puede configurar para variar en un intervalo de tiempo predeterminado, tal como cada 5 segundos. Esta variación en los datos de autenticación reduce la oportunidad de que un adversario lea la misma información de la RFID en una etapa posterior. Dependiendo de la

configuración del algoritmo de autenticación, el receptor puede tener que sincronizarse con el remitente, lo que hace aún más difícil para un adversario potencial obtener acceso no autorizado a un dispositivo móvil 105.

Con referencia de nuevo al bloque 305 de la figura 3, en otro ejemplo, los datos de autenticación intercambiados por el canal secundario 415 pueden ser codificados por información en un código de barras. Con este ejemplo, el lector 430 del segundo dispositivo puede ser un director de código de barras, tal como una cámara, escáner, láser o dispositivo similar para capturar información de códigos de barras. Cada vez más, los dispositivos móviles 105 están equipados con cámaras. Esta tendencia continuará probablemente ya que los proveedores de dispositivos móviles 105 continúan intentando agregar más funcionalidades. Tales cámaras se pueden usar para capturar una imagen del código de barras de manera que los datos de autenticación codificados en el código de barras se puedan decodificar y utilizar para determinar si la parte asociada con el código de barras es una parte de confianza. Como se describe para el ejemplo RFK, el dispositivo móvil 105 puede estar configurado para procesar los datos de autenticación descodificados desde el código de barras usando cualquier número de algoritmos de autenticación diferentes.

Típicamente, para capturar una imagen de un código de barras, se requiere que el receptor - el segundo dispositivo 410 en el ejemplo de la figura 4 - esté dentro de la proximidad física del código de barras. Con las cámaras convencionales, esto es típicamente posible en un rango de aproximadamente 1 metro o menor. Por consiguiente, la proximidad física del canal secundario 415 se realiza cuando la cámara captura una imagen del código de barras. En este ejemplo, el canal secundario 415 es un canal óptico que utiliza una línea de visión visual en oposición al canal de radiofrecuencia que se ha descrito para el ejemplo de la RFID. El código de barras que codifica los datos de autenticación puede ser un código de barras unidimensional o bidimensional. Una diferencia entre los códigos de barras unidimensionales y bidimensionales es que estos últimos son más fáciles de leer con cámaras de baja calidad como las que se aplican en dispositivos móviles.

Un código de barras puede codificar una cantidad suficiente de datos de autenticación para que la parte receptora no esté obligada a almacenar datos adicionales para autenticar a las partes. Se debe apreciar, sin embargo, que el esquema de codificación particular se puede variar como cuestión de elección de diseño y que el procesamiento subsiguiente de datos descodificados a partir del código de barras se puede variar dependiendo de la aplicación particular.

En una realización ilustrativa, el código de barras puede estar grabado permanentemente en un medio físico, tal como una tarjeta de plástico (por ejemplo, una tarjeta de crédito) que puede ser transportada por el usuario. En otro ejemplo, el código de barras puede estar grabado en relieve en el dispositivo móvil 105 de un usuario. En otra realización más, el código de barras se puede generar electrónicamente en la pantalla del dispositivo móvil 105.

Haciendo referencia a la figura 5, se muestra una representación simplificada de un dispositivo móvil 105. En este ejemplo, el dispositivo móvil 105 está equipado con una pantalla 500. La mayoría de los dispositivos móviles, si no todos, incluyen una pantalla como parte de su interfaz de usuario. La pantalla 500 se puede usar para presentar un código de barras 505 para la lectura por otra parte. Es decir, el código de barras 505 se puede presentar en la pantalla 500 mientras el dispositivo móvil 105 está en proximidad del lector 430 (por ejemplo, cámara) de otra parte. Cuando se activa la cámara de la parte lectora, se captura una imagen del código de barras 505, transfiriendo así los datos de autenticación codificados por el canal secundario 415.

Cuando se presentan en una pantalla, los códigos de barras se pueden cambiar fácilmente de manera regular. De forma similar a las RFID variables, el cambio periódico de códigos de barras de acuerdo con un programa predeterminado o de forma aleatoria añade un mecanismo de seguridad adicional para frustrar a posibles adversarios. Esto es especialmente cierto si el algoritmo de autenticación está diseñado de tal manera que las partes deben estar sincronizadas para que el emparejamiento tenga éxito.

Con el canal secundario 415, se pueden ignorar otros dispositivos móviles 105 que intentan emparejarse usando solamente el canal primario 400. Debido a que ambas partes 405, 410 involucradas en el proceso de autenticación están en proximidad física, se establece una relación de confianza explícita. Es decir, debido a la proximidad física de los dispositivos, ambas partes 405, 410 pueden ver físicamente con quién se están emparejando. La proximidad física es reforzada por la naturaleza de corto alcance del canal secundario 415 independientemente de la tecnología empleada (por ejemplo, RFID, códigos de barras, etc.)

Si las partes 405, 410 desean mantener la proximidad física necesaria para la autenticación, el canal secundario 415 se puede utilizar para intercambiar otra información, mientras la conexión exista. Debido a la naturaleza de corto alcance del canal secundario 415, se puede esperar, sin embargo, que esta conexión exista sólo durante un tiempo corto.

REIVINDICACIONES

1. Un procedimiento para autenticar un dispositivo móvil (105), **CARACTERIZADO PORQUE** el procedimiento comprende:

recibir una solicitud de comunicación (300) desde el dispositivo móvil (105), en el que el dispositivo móvil (105) es operativo para intercambiar datos a través de un canal primario (400), y en el que la solicitud de comunicación (300) se recibe usando el canal primario (400), siendo el canal primario uno de entre: un canal infrarrojo, un canal IEEE 802.3, un canal Ethernet, un canal de acceso múltiple de división de código, CDMA, un canal Bluetooth o un canal de sistema global para comunicación móvil, GSM; y a continuación

recibir datos de autenticación (305) desde el dispositivo móvil (105) por un canal secundario (415), en el que el canal secundario (415) es un canal de corto alcance operativo para intercambiar datos cuando el dispositivo móvil (105) está dentro de una proximidad física, siendo el canal secundario uno de entre un canal de identificación de radiofrecuencia o un canal óptico; y

procesar los datos de autenticación (310) para determinar si el dispositivo móvil (105) es un dispositivo de confianza.

2. El procedimiento de la reivindicación 1, en el que la solicitud de comunicación (300) es recibida por un segundo dispositivo móvil (105), y el canal secundario (415) es un canal de móvil a móvil entre el primer y segundo dispositivos móviles (105).

3. El procedimiento de la reivindicación 2, en el que los datos de autenticación son procesados por el segundo dispositivo móvil (105) para emparejar el primer y segundo dispositivos móviles (105).

4. El procedimiento de la reivindicación 1, en el que si el canal secundario es un canal de identificación de radiofrecuencia, el canal secundario (415) puede operar para intercambiar los datos de autenticación en una distancia de aproximadamente 1 m o menor.

5. El procedimiento de la reivindicación 4, en el que los datos de autenticación son una etiqueta de identificación por radiofrecuencia (RFID).

6. El procedimiento de la reivindicación 5, en el que la RFID varía de acuerdo con un intervalo de tiempo predeterminado.

7. El procedimiento de la reivindicación 1, en el que si el canal secundario es un canal óptico, el canal secundario (415) es operativo para intercambiar los datos de autenticación en una distancia de aproximadamente 1 metro o menor.

8. El procedimiento de la reivindicación 7, en el que los datos de autenticación incluyen datos codificados en un código de barras (505), y recibir los datos de autenticación comprende además capturar una imagen del código de barras (505) usando un lector.

9. El procedimiento de la reivindicación 8, en el que el código de barras (505) se genera electrónicamente y se presenta en una pantalla del dispositivo móvil (105).

10. El procedimiento de la reivindicación 8, en el que el código de barras (505) está grabado permanentemente en el dispositivo móvil (105).

11. Un sistema para autenticar un dispositivo móvil, estando configurado el sistema para:

recibir una solicitud de comunicación (300) desde el dispositivo móvil (105), en el que el dispositivo móvil (105) es operativo para intercambiar datos a través de un canal primario (400), y en el que la solicitud de comunicación (300) se recibe usando el canal primario (400), siendo el canal primario uno de entre: un canal infrarrojo, un canal IEEE 802.3, un canal Ethernet, un canal de acceso múltiple de división de código, CDMA, un canal Bluetooth o un canal de sistema global para comunicación móvil, GSM; y a continuación

recibir datos de autenticación (305) desde el dispositivo móvil (105) por un canal secundario (415), en el que el canal secundario (415) es un canal de corto alcance operativo para intercambiar datos cuando el dispositivo móvil (105) está dentro de la proximidad física, siendo el canal secundario uno de entre un canal de identificación de radiofrecuencia o un canal óptico; y

procesar los datos de autenticación (310) para determinar si el dispositivo móvil (105) es un dispositivo de confianza.

12. Un dispositivo móvil para la autenticación con un segundo dispositivo, siendo operativo el dispositivo móvil (105) para intercambiar datos a través de un canal primario, estando configurado el dispositivo móvil para: enviar una solicitud de comunicación (300) utilizando el canal primario (400), siendo el canal primario uno de entre: un canal infrarrojo, un canal IEEE 802.3, un canal Ethernet, un canal de acceso múltiple de división de código, CDMA, un canal Bluetooth o un canal de sistema global para comunicación móvil, GSM;

y a continuación enviar datos de autenticación (305) por un canal secundario (415) a un segundo dispositivo, en el que el canal secundario (415) es un canal de corto alcance operativo para intercambiar datos cuando el dispositivo móvil (105) está dentro de la proximidad física del segundo dispositivo, siendo el canal secundario uno de entre un canal de identificación de radiofrecuencia o un canal óptico.

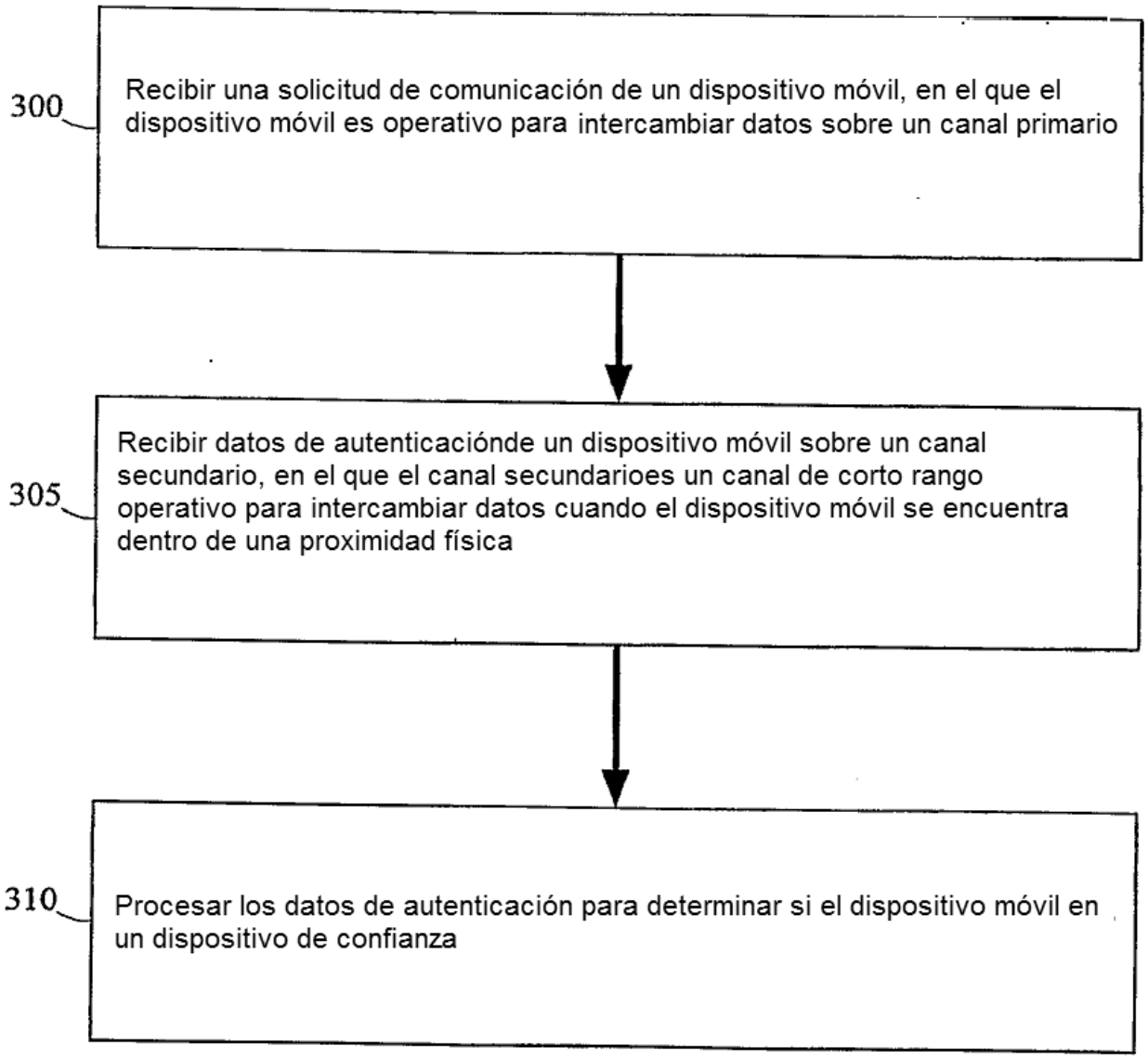
300
Recibir una solicitud de comunicación de un dispositivo móvil, en el que el dispositivo móvil es operativo para intercambiar datos sobre un canal primario
305
Recibir datos de autenticaciónde un dispositivo móvil sobre un canal secundario, en el que el canal secundarioes un canal de corto rango operativo para intercambiar datos cuando el dispositivo móvil se encuentra dentro de una proximidad física
310
Procesar los datos de autenticación para determinar si el dispositivo móvil en un dispositivo de confianza

FIGURA 3

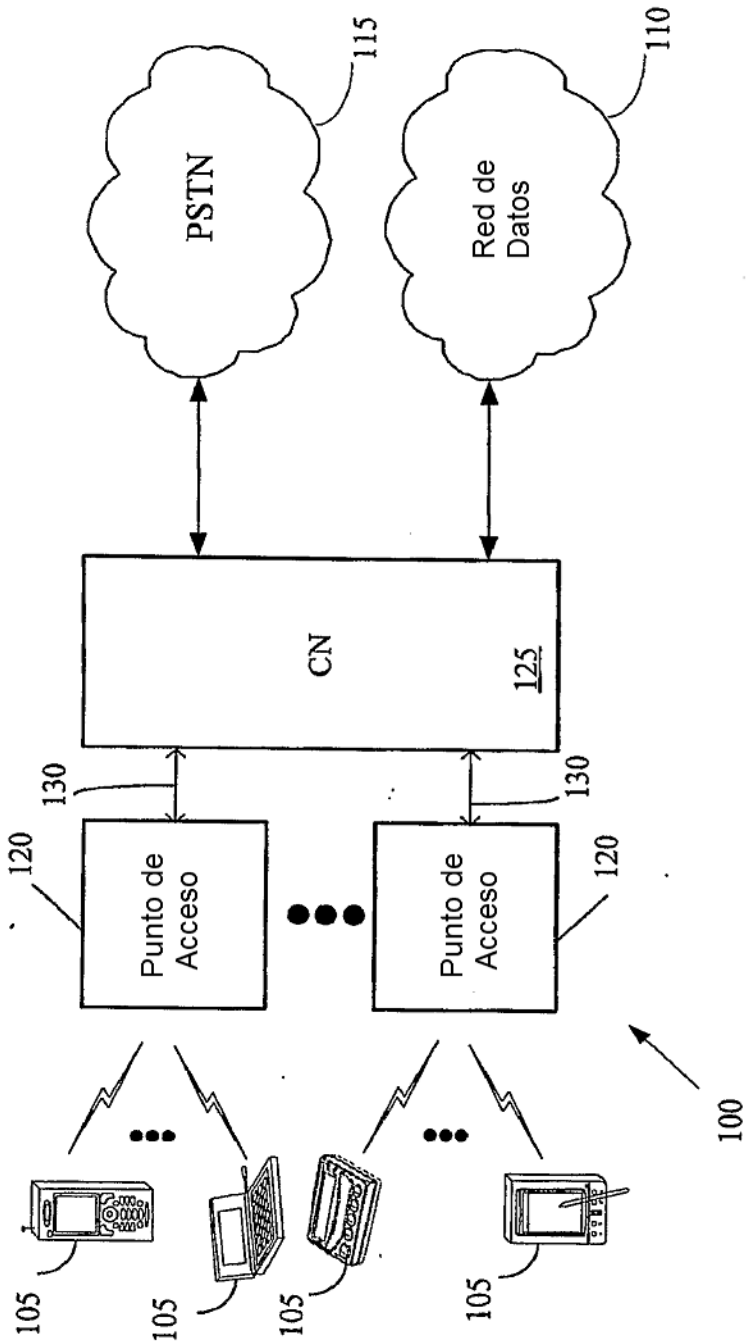

FIGURA 1

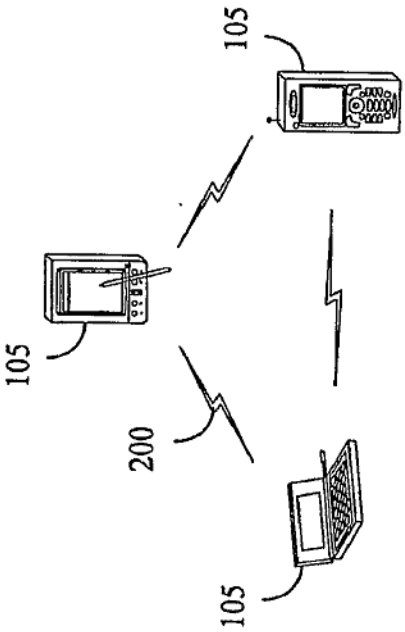

FIGURA 2

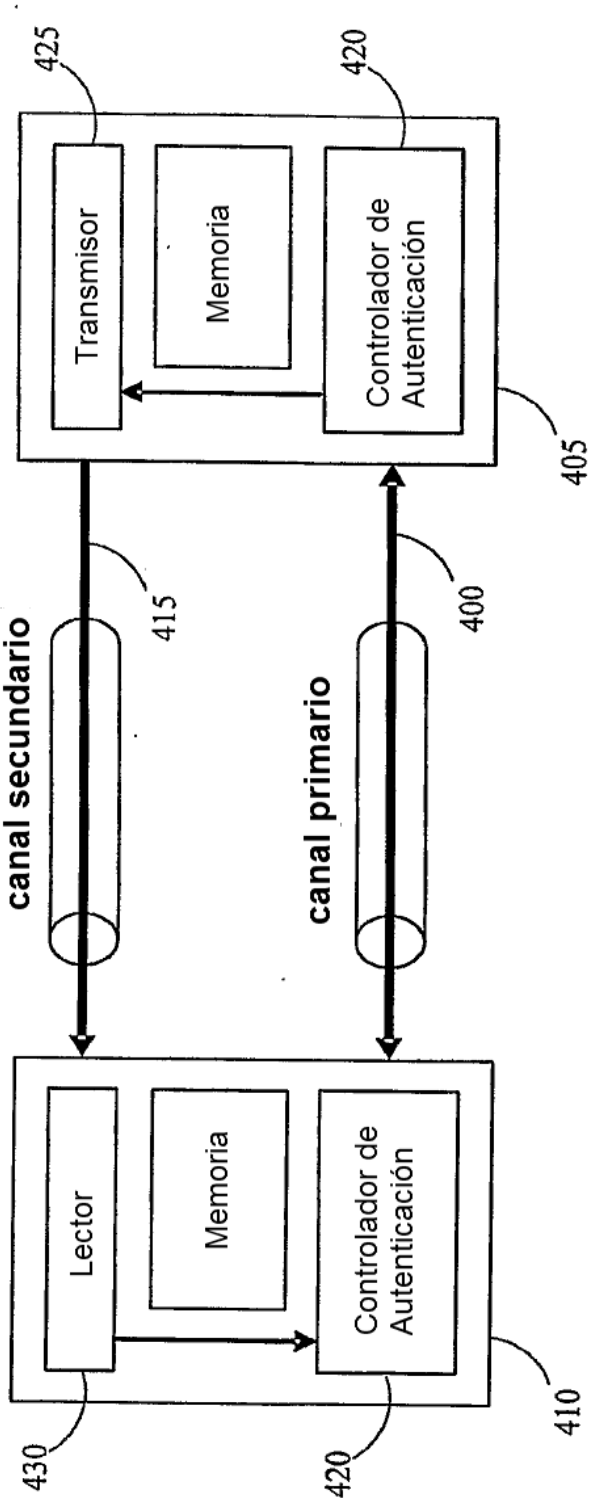

FIGURA 4

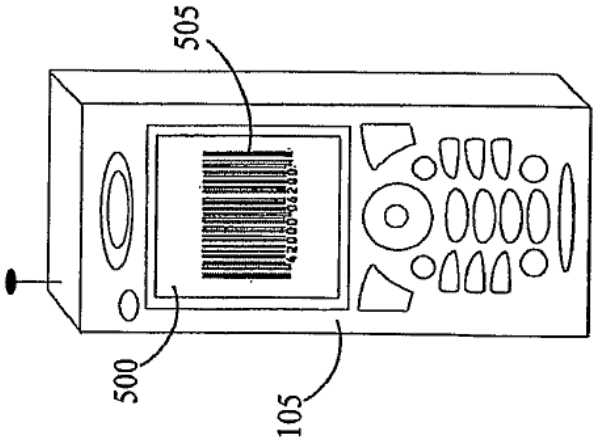

FIGURA 5