(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 937 644**

(51) Int. CI.:

H04L 9/40 (2012.01)
H04W 12/06 (2011.01)
H04W 84/12 (2009.01)
H04W 12/50 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.01.2007 E 17165974 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2023 EP 3223489**

(54) Título: **Procedimiento para la 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:
30.03.2023

(73) Titular/es:

NOKIA OF AMERICA CORPORATION (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:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Procedimiento para la autenticación segura de dispositivos móviles

Antecedentes de la invención

Campo de la invención

Esta invención se refiere generalmente a sistemas de comunicación y, más particularmente, a sistemas de comunicación inalámbrica.

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 se componen generalmente de colecciones heterogéneas de tecnologías de interfaz aérea, 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 área local y redes de "punto de conexión", conectividad Bluetooth, redes IEEE-802.16 (WiMax) que proporcionan acceso fijo inalámbrico y móvil de banda ancha, redes optimizadas de datos de evolución (1xEVDO) que proporcionan acceso a usuarios de datos móviles de tercera generación (3G), y similares.

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

En entornos públicos, por ejemplo, tal como un terminal de aeropuerto, adversarios pueden intentar escuchar furtivamente en comunicaciones inalámbricas 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 similares. Adversarios pueden usar esta información para obtener acceso no autorizado a sistemas de comunicación inalámbrica y/u otros dispositivos móviles. Para ilustrar este punto, en el caso del protocolo Bluetooth, un adversario puede escuchar furtivamente durante el emparejamiento de dispositivos móviles. Como se usa en esta invención, los términos "autenticaciones", "autenticar", "emparejamiento" y "emparejarse" están destinadas a usarse de manera intercambiable para referirse generalmente a algoritmos, procedimientos, mecanismos y/o datos utilizados para establecer comunicaciones confiables. Durante el procedimiento de emparejamiento, el adversario puede "escuchar" para interceptar el o los PIN de uno o más dispositivos móviles. Con esta información, el adversario puede decodificar los 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, como datos de calendario, libros de direcciones, correo electrónico, información de tarjetas de crédito y similares.

Un algoritmo de ataque ilustrativo se describe, por ejemplo, en un artículo titulado "Cracking the Bluetooth PIN" por Yaniv Shaed y Avishai Wool; cuyo contenido se incorpora aquí como referencia. En este artículo, con respecto al protocolo Bluetooth, los autores describen una deficiencia que existe en función únicamente de un PIN de n-dígitos para emparejar un dispositivo móvil con otro. En particular, los autores describen un algoritmo que puede usarse con un PIN interceptado de un dispositivo móvil para "craquear" mecanismos de autenticación Bluetooth convencionales en menos de un segundo. Otros protocolos utilizados en diferentes tecnologías inalámbricas, tales como Wi-Fi, 1xEVDO, y similares, sufren deficiencias similares en que los adversarios han demostrado éxito en interceptar datos de autenticación y usar estos datos para obtener acceso no autorizado a datos confidenciales.

Lo que se necesita, por lo tanto, es un mecanismo de autenticación que, cuando se utilice, garantice mejor que solo se permita que los dispositivos móviles confiables se emparejen entre sí y/o intercambien datos con una red de comunicación inalámbrica.

El documento US-2005221813 se refiere a utilizar una primera interfaz de comunicación predeterminada (celular) para iniciar comunicaciones a través de una segunda interfaz de comunicación auxiliar (Bluetooth, Wi-Fi); la política y la información de autenticación se envían desde el iniciador hasta la diana a través de un enlace predeterminado.

El documento US-2003119568 se refiere a un sistema activo que usa un transmisor de activación complementario para enviar señales de RF y datos que incluyen un código de identificador para excitar un receptor de activación complementario. Filtro compara el código con un código almacenado y si coinciden, activa otros componentes del dispositivo. Si los códigos de ID no coinciden no se toma ninguna acción adicional. El receptor de activación inalámbrica activa entonces el transceptor de comunicación bidireccional inalámbrica (Bluetooth, Wi-Fi) y ambas partes pueden establecer comunicación.

El documento US-2003200434 se refiere a un procedimiento de identificación automático llevado a cabo colocando los dos dispositivos muy próximos entre sí, y transmitiendo señales de intervalo muy cortos desde el aparato maestro, para recibirse exclusivamente por el aparato esclavo. Si los dos dispositivos pueden comunicarse a través de este corto intervalo, se genera una clave de identificación y se pasa al aparato esclavo para intercambios posteriores en comunicaciones normales, de intervalo más grande.

El documento WO2004090800A2 se refiere a un aparato, así como a un procedimiento para determinar de manera fiable el uso deliberado de una portadora de datos sin contacto. El término "portadora de datos sin contacto" usado en el documento WO2004090800A2 se refiere a todas las disposiciones, que tienen un microchip y una antena conectadas a ella y están adaptadas para intercambiar datos con un dispositivo de lectura adecuado. Estos incluyen, al lado de tarjetas de chip para aplicaciones de pago, documentos de identificación legibles por contacto, tales como pasaportes y tarjetas de identidad con microchip incorporado, así como también etiquetas de RFID. Se puede emplear un canal de transmisión de datos basado en antenas en dependencia de los datos a transmitir adicionalmente un canal óptico de transmisión de datos entre el dispositivo de lectura y la portadora de datos sin contacto. Con la ayuda del canal de transmisión de datos adicional mediante medios ópticos se intercambian datos entre el dispositivo de lectura y la portadora de datos, que son adecuados para realizar una autenticación entre el dispositivo de lectura y la tarjeta sin contacto. La autenticación a través del canal de transmisión de datos adicional evita una activación involuntaria de la tarjeta sin contacto, ya que la información óptica no está disponible, cuando el portador de datos no es ópticamente visible al dispositivo de lectura, por ejemplo, se transporta en una bolsa/bolso. Por ejemplo, la portadora de datos tiene información legible ópticamente, tal como, por ejemplo, un código de barras o código de matriz. Cuando la tarjeta se presenta al dispositivo de lectura, esta información se lee y evalúa por medio de un dispositivo de lectura óptica, por ejemplo, un escáner de códigos de barras. La información de lectura óptica puede usarse entonces por la portadora de datos sin contacto para autenticar propósitos entre sí mismos y el dispositivo de lectura sin contacto, para que de tal manera proporcione la autorización para una transacción posterior.

La presente invención está dirigida a abordar los efectos de uno o más de los problemas expuestos anteriormente.

Resumen de la invención

Este objeto se resuelve mediante la invención según reivindicado en las reivindicaciones independientes. Las realizaciones preferidas se definen en las reivindicaciones dependientes.

Breve descripción de las figuras

La invención puede entenderse por referencia a la siguiente descripción tomada junto con los dibujos adjuntos, en los que números de referencia similares identifican elementos similares, y en los 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 móvil a móvil entre uno o más dispositivos móviles;

La Figura 3 ilustra conceptualmente un procedimiento para autenticar 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 mostrado en la Figura 3 de acuerdo con una realización de la presente invención.

Aunque la invención es susceptible de diversas modificaciones y formas alternativas, se han mostrado realizaciones específicas de la misma a modo de ejemplo en los dibujos y se describen en detalle en esta invención.

Descripción detallada de realizaciones específicas

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. Se apreciará, por supuesto, que en el desarrollo de cualquier realización real, deben hacerse numerosas decisiones específicas de implementación para lograr los objetivos específicos de los desarrolladores, tales como el cumplimiento de restricciones relacionadas con el sistema y relacionadas con el negocio, que variarán de una implementación a otra. Además, se apreciará que tal esfuerzo de desarrollo podría ser complejo y llevar mucho tiempo, pero, sin embargo, sería una rutina de los expertos en la técnica que tiene el beneficio de esta descripción.

Las partes de la presente invención y la descripción detallada correspondiente se presentan en términos de software, o algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de una memoria de ordenador. Estas descripciones y representaciones son las por las que los expertos en la técnica transmiten eficazmente la sustancia de su trabajo a otros expertos en la técnica. Un algoritmo, como el término se usa aquí, y como se usa en general, se concibe que sea una secuencia autoconsistente de etapas que conducen a un resultado deseado. Las

etapas son aquellas que requieren manipulaciones físicas de cantidades físicas. Por lo general, aunque no necesariamente, estas cantidades toman la forma de señales ópticas, eléctricas o magnéticas capaces de almacenarse, transferirse, combinarse, compararse y manipularse de otro modo. Se ha demostrado conveniente en ocasiones, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

Sin embargo, debe tenerse en cuenta que todos estos términos y términos similares deben asociarse con las cantidades físicas apropiadas y son simplemente etiquetas convenientes aplicadas a estas cantidades. A menos que se indique específicamente lo contrario, o como es evidente a partir de la discusión, términos tales como "procesamiento" o "calcular" o "cálculo" o "determinar" o "visualizar" o similares, se refieren a la acción y a los procedimientos de un sistema informático, o dispositivo informático electrónico similar, que manipula y transforma datos representados 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 del sistema informático o registros u otros tales dispositivos de almacenamiento, transmisión o visualización de información.

Obsérvese 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 programa puede ser magnético (por ejemplo, un disquete o un disco duro), óptico (por ejemplo, una memoria de solo lectura de disco compacto, o "CD ROM"), o en base a otras tecnologías y puede ser de solo lectura o de acceso aleatorio. De manera similar, el medio de transmisión puede ser pares de cables retorcidos, 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 cualquier implementación dada.

La presente invención se describirá ahora con referencia a las figuras adjuntas. Varias estructuras, sistemas y dispositivos se representan esquemáticamente en los dibujos con fines de explicación solamente y para no complicar 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 usadas en esta invención deben entenderse e interpretarse para tener un significado consistente con la comprensión de esas palabras y frases por los expertos en la técnica pertinente. No se pretende que la definición especial de un término o frase, es decir, una definición diferente del significado ordinario y habitual, como se entiende por los expertos en la técnica, se implemente mediante el uso consistente del término o expresión en esta invención. En la medida en que se pretende que un término o frase tenga un significado especial, *a saber,* un significado distinto de los entendidos por los expertos en la técnica, tal definición especial se expondrá expresamente en la especificación de manera definitiva que proporciona directa e inequívocamente la definición especial para el término o expresión.

Volviendo ahora a los dibujos, y con 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 esta invención para describir generalmente una red de comunicación que es operable para proporcionar comunicación móvil a sus abonados. Por ejemplo, la red de comunicación inalámbrica 100 puede ser una red 1xEVDO que generalmente cumple con las especificaciones técnicas y los informes técnicos para un Sistema Móvil de 3ª Generación que ha sido desarrollado por un Proyecto de Asociación de 3ª Generación (3GPP). Sin embargo, debe entenderse que la presente invención puede ser aplicable a redes de comunicación inalámbrica que soportan otros protocolos inalámbricos, tales como Wi-Fi, Bluetooth, WiMax, y similares.

La red de comunicación inalámbrica 100 permite que uno o más dispositivos móviles 105 se comuniquen con una red de datos 110, tal como Internet, y/o una Red Telefónica Conmutada Pública (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 tomar 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 se puede acoplar a una red central (CN) 125 mediante una o más conexiones 130, tales como líneas o circuitos T1/EI, circuitos de ATM, cables, líneas de abonado digital (DSL) y similares. Además, la red de comunicación 100 puede comprender otros dispositivos (no mostrados), tales como controladores de red de radio (RNC), procesadores de gestión y similares.

Generalmente, la CN 125 funciona como una interfaz a una red de datos 110 y/o a la PSTN 115. La CN 125 puede realizar una variedad de funciones y operaciones, tales como la autenticación de usuario. Sin embargo, como se describirá más detalladamente a continuación, el procedimiento de autenticar un dispositivo móvil 105 para la comunicación confiable puede realizarse por cualquier número de dispositivos en la red de comunicación 100, tal como el punto de acceso 120 u otros dispositivos (no mostrados). Además, para comunicaciones de móvil a móvil (por ejemplo, maestro/esclavo, entre pares, etc.), el procesamiento de autenticación puede realizarse por uno o más dispositivos móviles 105. Por lo tanto, se apreciará que una descripción detallada de la estructura y el funcionamiento de la CN 125 no es necesaria para comprender y apreciar la presente invención. Por consiguiente, para evitar innecesariamente ofuscar la presente invención, los detalles adicionales de la CN 125 no se presentan en esta invención.

Los expertos en la materia 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. Sin embargo, debe entenderse que la configuración

de la red de comunicación inalámbrica 100 es de naturaleza ejemplar, y que pueden emplearse menos componentes o componentes adicionales en otras realizaciones del sistema de comunicaciones 100 sin apartarse del alcance de la presente invención.

La Figura 2 ilustra la comunicación móvil a móvil entre una pluralidad de dispositivos móviles 105. Aunque solo se ilustran tres dispositivos móviles 105 para este ejemplo particular, debe apreciarse que la comunicación 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 también pueden estar en comunicación de datos con una red de comunicación, tal como la red de comunicación 100 ilustrada en la Figura 1. Cuando uno o más dispositivos móviles 105 están en comunicación de datos con una red de comunicación, debe apreciarse que, bajo ciertas configuraciones, otros dispositivos móviles 105 pueden comunicarse (por ejemplo, intercambiar datos) con la red de comunicación, a través de la comunicación móvil a móvil.

La comunicación móvil a móvil puede implementarse usando cualquier número de tecnologías y protocolos inalámbricos conocidos o desarrollados. En la Figura 2, los dispositivos móviles 105 se muestran comunicándose a través de un canal primario 200. El canal primario 200 es un canal de radiofrecuencia.

Con referencia a la Figura 3, se muestra un procedimiento para autenticar un dispositivo móvil 105 de acuerdo con una realización de la presente invención. Para facilitar la descripción, el procedimiento se describe con referencia a la red de comunicación 100 y la comunicación móvil a móvil mostrada en las Figuras 1 y 2, respectivamente. Sin embargo, debe apreciarse que el procedimiento es igualmente aplicable a otras redes inalámbricas y configuraciones móvil a móvil.

En el bloque 300, se recibe una solicitud de comunicación desde un dispositivo móvil 105. Como se describe, el dispositivo móvil 105 es operable para comunicarse a través de un canal primario 200. El canal primario 200 es el canal de comunicación de datos previsto para una tecnología inalámbrica dada y, típicamente, proporciona al dispositivo móvil 105 cierta libertad de movimiento, mientras se mantiene la comunicación de datos. En una red Wi-Fi, por ejemplo, el canal primario es normalmente 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.

Con 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 el primer como el segundo dispositivo 405, 410 son dispositivos móviles, y el canal primario 400 es un canal de comunicación móvil a móvil. En otra realización ilustrativa, solo uno de los dispositivos 405, 410 es un dispositivo móvil, y el otro es un punto de acceso a una red de comunicación. Además, debe apreciarse que dispositivos electrónicos adicionales (no mostrados) también pueden ser capaces de comunicarse con el primer y segundo dispositivos 405, 410 usando el canal primario 400.

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

En el diagrama de bloques simplificado mostrado en la Figura 4, que ilustra el procedimiento de autenticación mostrado en la Figura 3 de acuerdo con una realización de la presente invención, 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 se genera normalmente por un dispositivo que desea iniciar la comunicación inalámbrica. Debe entenderse que la solicitud de comunicación puede generarse 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. Normalmente, la solicitud incluye datos que se reconocerán e interpretarán como una solicitud de comunicación. Además, la solicitud de comunicación se transmite a través del canal primario 400. Como se describe, el canal secundario 415 es un canal de corto alcance que utiliza proximidad física para intercambiar datos, mientras que, en relación con el canal secundario 415, el canal primario 400 es un canal de intervalo más largo que permite una mayor movilidad física.

Con referencia de nuevo a la Figura 3, en el bloque 305, los datos de autenticación se reciben desde el dispositivo móvil 105 a través del canal secundario 415. Como se describe, el canal secundario 415 es un canal de corto alcance que se basa en una proximidad física para intercambiar datos. A diferencia del canal 400 primario, que permite una mayor distancia de separación, el canal 415 secundario requiere que el dispositivo móvil se coloque próximo al

dispositivo que está intentando autenticarse. Esta proximidad física hace que sea más difícil, si no imposible, que un adversario se empareje con otra parte sin detección. Esto se debe a que, durante el procedimiento de búsqueda, el adversario ya no puede depender del canal primario 400 para mantener una distancia segura de su diana.

En una realización ilustrativa, el canal secundario 415 se realiza usando tecnología de identificación por radiofrecuencia (RFID). Una ventaja de la RFID es que no requiere un contacto directo o un barrido de línea de visión, sino que se basa en la ventaja física de proximidad descrita para el canal secundario 415. Con referencia a la Figura 4, en el caso ilustrativo de RFID, el primer dispositivo 405 puede estar equipado con una etiqueta de RFID (no mostrada). En este ejemplo, la etiqueta de RFID puede formar parte de un controlador de autenticación 420. Sin embargo, debe apreciarse que el controlador de autenticación 420 y otros componentes mostrados para el primer y segundo dispositivos 405 y 410 están previstos para fines ilustrativos y no limitativos. Los expertos en la materia apreciarán que la funcionalidad descrita en esta invención puede configurarse para ser operable con menos o más de los componentes mostrados en las figuras adjuntas y que la configuración real del sistema puede variar como una cuestión de elección de diseño.

La etiqueta de RFID puede ser activa o pasiva. Una etiqueta RFID activa está normalmente asociada con su propia fuente de alimentación, mientras que las etiquetas pasivas son etiquetas RFID sin una fuente de alimentación. Las etiquetas pasivas se activan temporalmente por el escaneo de radiofrecuencia de un lector. Sin embargo, la configuración y el funcionamiento particulares de las etiquetas 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 con la etiqueta de RFID a otro dispositivo. Cuando se activa, la etiqueta de RFID suele generar 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 es normalmente menor que las tecnologías inalámbricas típicas, tales como Bluetooth, Wi-Fi y similares. Con RFID pasiva, por ejemplo, el canal secundario 415 utilizado para transmitir datos de RFID (es decir, datos de autenticación) es típicamente de aproximadamente 1 metro o menos. En el caso de Bluetooth, el canal primario es normalmente de alrededor de 10 metros. Por consiguiente, la RFID obliga a la proximidad física deseada para reducir o posiblemente eliminar el emparejamiento no autorizado. En la práctica, por ejemplo, para un usuario con un dispositivo móvil 105 equipado con una etiqueta de RFID, sería necesario sujetar físicamente su dispositivo móvil 105 aproximadamente 50 cm o más cerca de la otra parte para leer/intercambiar datos de RFID. Sería difícil, si no imposible, para un adversario, llegar dentro de dicha proximidad física cercana y aún así evitar ser detectado. En otro ejemplo ilustrativo, ambas partes 405 y 410 están configuradas con etiquetas 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 confiables.

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 confiable (es decir, determinar si es un dispositivo autorizado que está intentando emparejarse). En el ejemplo de RFID anterior, la etiqueta RFID genera los datos de autenticación, que, como se describe, pueden incluir datos de identificación. Los datos de identificación pueden incluir cualquier cadena binaria de datos operable 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 puede configurarse para determinar si es un dispositivo confiable que está intentando emparejarse. En un ejemplo ilustrativo, los datos de autenticación pueden usarse como una entrada de parámetro en un algoritmo de autenticación programado en el controlador de autenticación 420. En otras palabras, la información de RFID puede usarse como una simiente para el procedimiento de emparejamiento. Después de procesar la información de RFID a través de su algoritmo de autenticación programado, el controlador de autenticación 420 puede determinar si se devuelve un resultado esperado. Si es así, el controlador de autenticación 420 determina que se comunica con un dispositivo confiable y permite que se complete el procedimiento de emparejamiento.

Debe apreciarse que la complejidad del algoritmo de autenticación usado para procesar los datos de autenticación (por ejemplo, información de RFID) 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 valores almacenados para determinar si existe una coincidencia. Si es así, el dispositivo de envío se considera un dispositivo confiable. En un caso complejo, los datos de autenticación intercambiados sobre el canal secundario 415 pueden configurarse para variar en ciertos intervalos, de modo que sirva como un número de ocasión (es decir, parámetro variable en el tiempo) para el algoritmo de autenticación. Por ejemplo, la información de RFID puede configurarse para variar en algún 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 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 que sea aún más difícil para un adversario ganar acceso no autorizado a un dispositivo móvil 105.

Alternativamente, el canal secundario 415 puede ser un canal óptico que usa línea visual de visión en oposición al canal de radiofrecuencia descrito para el ejemplo de RFID.

Con el canal secundario 415, otros dispositivos móviles 105 intentan emparejarse usando solo el canal primario 400 pueden ser ignorados. Debido a que ambas partes 405, 410 involucradas en el procedimiento 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 forzada por la naturaleza de corto alcance del canal secundario 415 independientemente de la tecnología empleada (por ejemplo, RFID, etc.)

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

Las realizaciones particulares descritas anteriormente son solo ilustrativas. Por consiguiente, la protección buscada en esta invención es como se expone en las reivindicaciones a continuación.

REIVINDICACIONES

1. Un procedimiento para la autenticación de un primer dispositivo móvil por un segundo dispositivo móvil, en donde los dispositivos móviles son operables para intercambiar datos a través de un canal primario, comprendiendo el procedimiento: enviar una solicitud de comunicación (300) desde un dispositivo móvil del primer y segundo dispositivos móviles al otro dispositivo móvil, del primer y segundo dispositivos móviles usando el canal primario (400); y luego enviar datos de autenticación (305) desde el primer dispositivo móvil a través de un canal secundario (415) al segundo dispositivo móvil, en donde el canal secundario (415) es diferente del canal primario y es un canal de corto alcance operable para intercambiar datos cuando el primer dispositivo móvil (105) está dentro de una proximidad física del segundo dispositivo móvil, en donde el canal primario (400), en relación con el canal secundario (415), es un canal de intervalo más largo que permite una mayor movilidad física, en donde el canal primario es un canal Bluetooth o un canal Wi-Fi.

2. El procedimiento de la reivindicación 1, en donde el canal secundario (415) es un canal móvil a móvil entre el primer y segundo dispositivos móviles (105).

3. El procedimiento de la reivindicación 2, en donde los datos de autenticación se procesan para emparejar los dos dispositivos móviles (105).

4. El procedimiento de cualquiera de las reivindicaciones 1 a 3, en donde el canal secundario es un canal de identificación por radiofrecuencia, RFID, operable para intercambiar los datos de autenticación entre una distancia de aproximadamente 1 m o menos.

5. El procedimiento de la reivindicación 4, en donde los datos de autenticación son datos de identificación por radiofrecuencia, RFID, asociados con una etiqueta de identificación por radiofrecuencia, RFID, del primer dispositivo móvil.

6. El procedimiento de la reivindicación 5, en donde los datos de RFID se varían según un intervalo de tiempo predeterminado.

7. El procedimiento de cualquiera de las reivindicaciones 1 a 6, el procedimiento comprende además procesar, por el segundo dispositivo móvil, los datos de autenticación (310) para determinar si el primer dispositivo móvil es un dispositivo confiable.

8. El procedimiento de la reivindicación 7, en donde el procesamiento comprende comparar los datos de autenticación con valores almacenados para determinar si existe una coincidencia.

9. El procedimiento de cualquiera de las reivindicaciones 7 y 8, en donde los datos de autenticación varían en ciertos intervalos de tiempo para servir como un parámetro variable en el tiempo para un algoritmo de autenticación.

10. El procedimiento de cualquiera de las reivindicaciones 1 a 9, en donde el primer dispositivo móvil y el segundo dispositivo móvil deben sincronizarse para que la autenticación sea exitosa.

11. Un primer dispositivo móvil operable para intercambiar datos con un segundo dispositivo móvil a través de un canal primario, en donde el primer dispositivo móvil comprende:

    - medios para recibir una solicitud de comunicación (300) desde el segundo dispositivo móvil usando el canal primario (400) o para enviar la solicitud de comunicación (300) al segundo dispositivo móvil usando el canal primario (400); y
    - medios para enviar, posteriormente, datos de autenticación (305) a través de un canal secundario (415) al segundo dispositivo móvil, en donde el canal secundario (415) es diferente del canal primario y es un canal de corto alcance operable para intercambiar datos cuando el primer dispositivo móvil (105) está dentro de una proximidad física del segundo dispositivo móvil,

    en donde el canal primario (400), en relación con el canal secundario (415), es un canal de intervalo más largo que permite una mayor movilidad física, en donde el canal primario es un canal Bluetooth o un canal Wi-Fi.

12. El primer dispositivo móvil según la reivindicación 11, en donde, si los datos de autenticación son datos de RFID asociados con la etiqueta de RFID del primer dispositivo móvil, el primer dispositivo móvil comprende un transmisor configurado para transmitir los datos de RFID asociados con la etiqueta de RFID del primer dispositivo móvil.

13. Un sistema que comprende:

    - el primer dispositivo móvil según cualquiera de las reivindicaciones 11 y 12; y

- el segundo dispositivo móvil.

14. El sistema de la reivindicación 13, en donde el segundo dispositivo móvil comprende:

- medios para procesar, por el segundo dispositivo móvil, los datos de autenticación (310) para determinar si el primer dispositivo móvil es un dispositivo confiable, en donde los datos de autenticación varían en ciertos intervalos de tiempo para servir como un parámetro variable en el tiempo para un algoritmo de autenticación.

15. El procedimiento de una de las reivindicaciones 13 y 14, en donde un dispositivo móvil del primer y segundo dispositivos móviles comprende un transmisor configurado para transmitir la solicitud de comunicación, y en donde el otro dispositivo móvil del primer y segundo dispositivos móviles comprende un receptor configurado para recibir la solicitud de comunicación.

16. El sistema de cualquiera de las reivindicaciones 13 a 15, en donde, si los datos de autenticación son datos de RFID asociados con la etiqueta de RFID del primer dispositivo móvil, el segundo dispositivo móvil comprende un lector configurado para recibir los datos de RFID asociados con la etiqueta de RFID del primer dispositivo móvil.

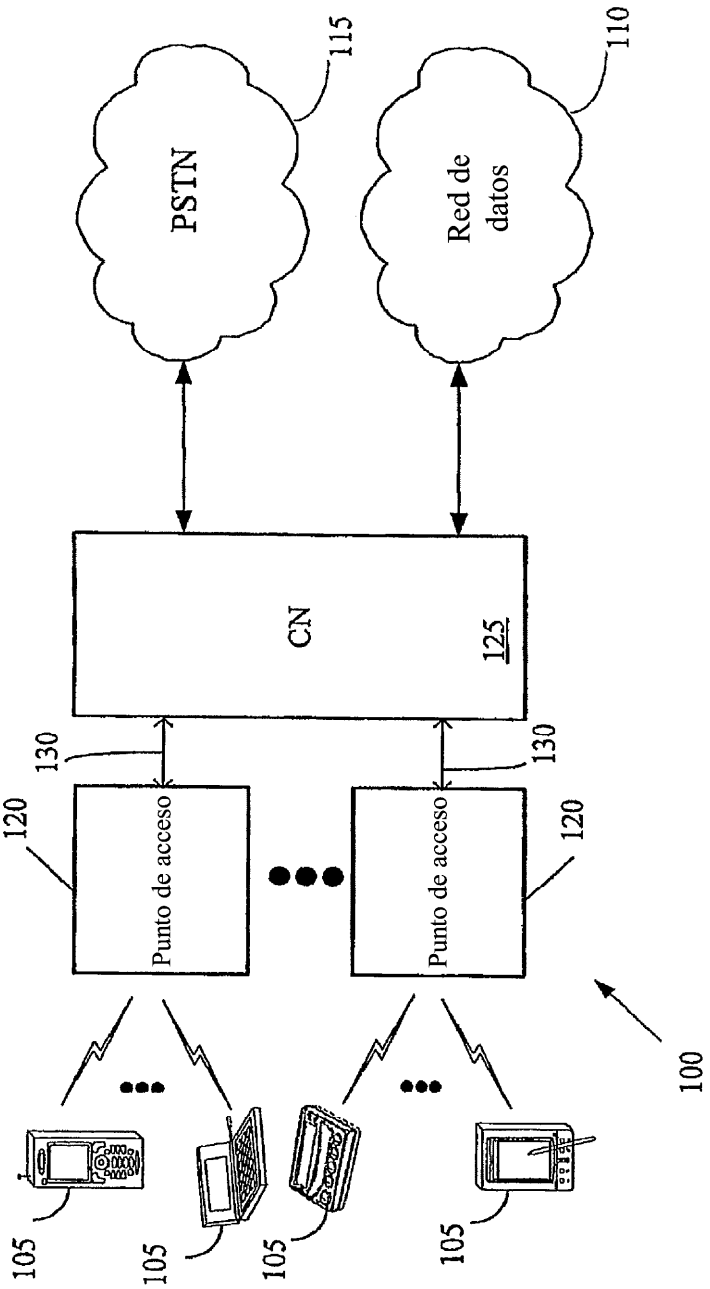

Figura 1

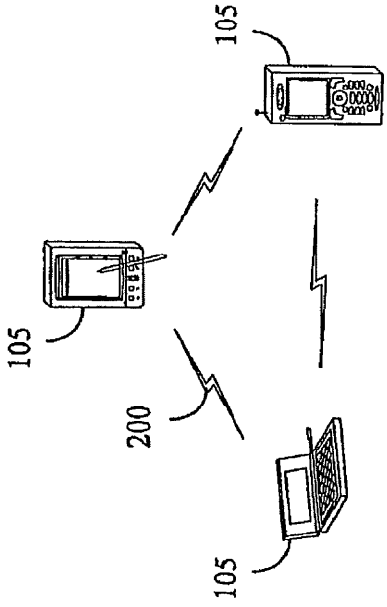

Figura 2

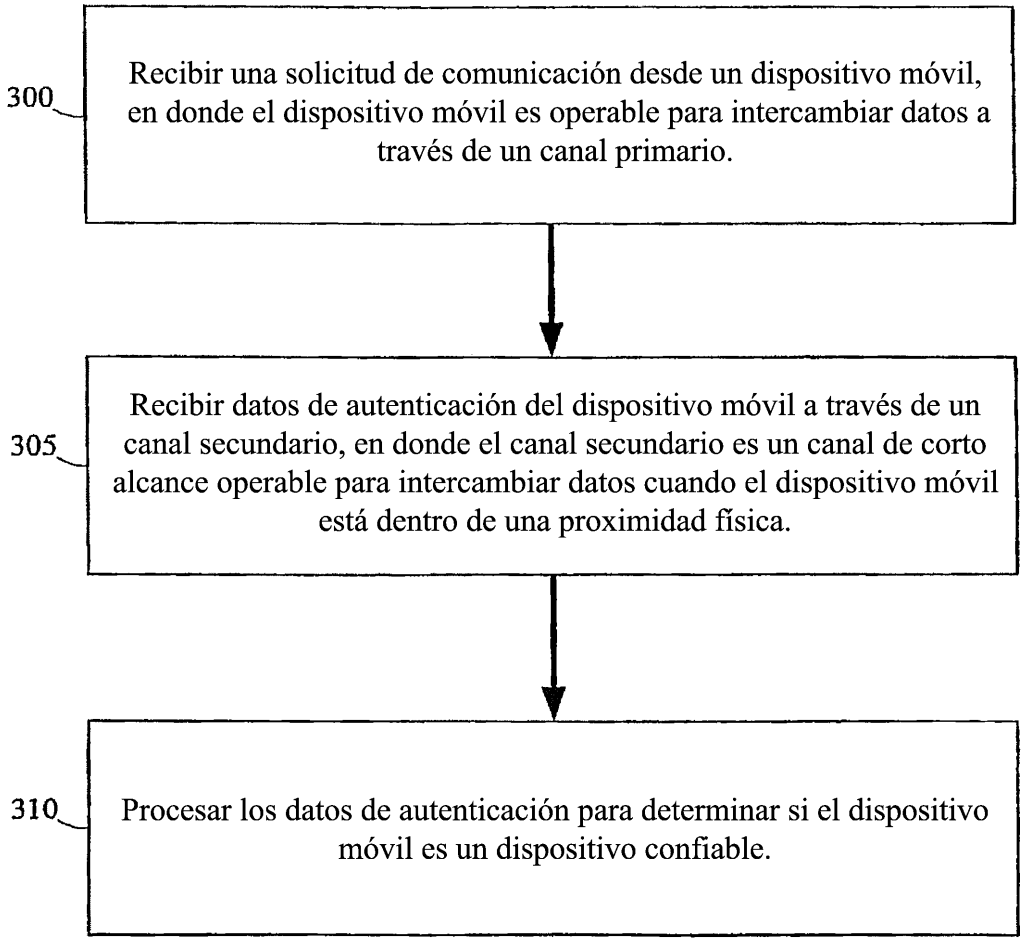
300
Recibir una solicitud de comunicación desde un dispositivo móvil, en donde el dispositivo móvil es operable para intercambiar datos a través de un canal primario.
305
Recibir datos de autenticación del dispositivo móvil a través de un canal secundario, en donde el canal secundario es un canal de corto alcance operable para intercambiar datos cuando el dispositivo móvil está dentro de una proximidad física.
310
Procesar los datos de autenticación para determinar si el dispositivo móvil es un dispositivo confiable.

Figura 3

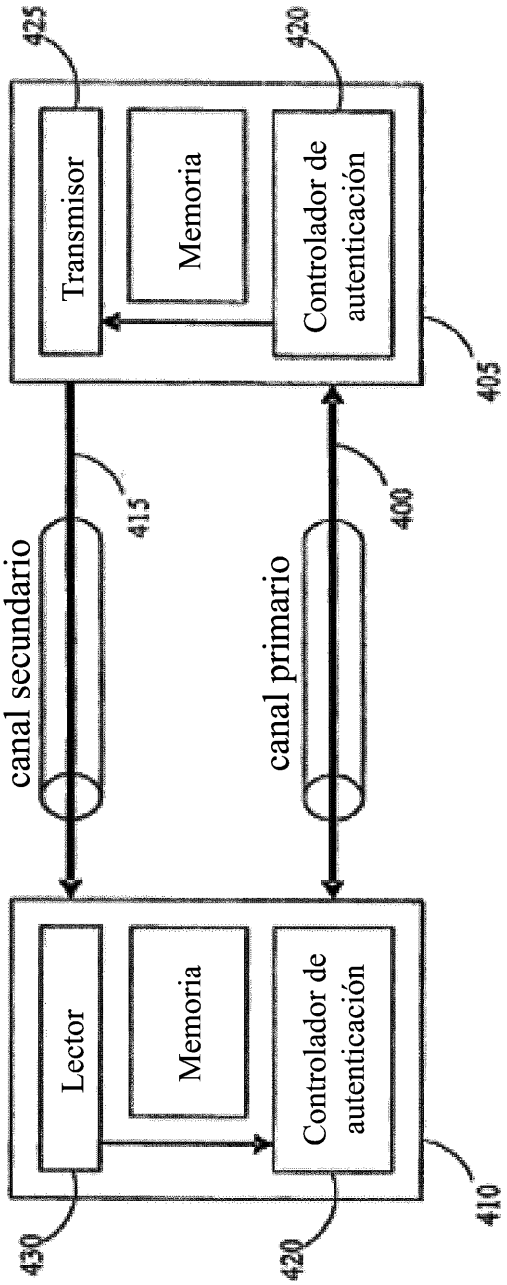
425
420
Transmisor
Memoria
Controlador de autenticación
405
415
400
canal secundario
canal primario
Lector
Memoria
Controlador de autenticación
410
430
420

Figura 4