



①9



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA

①1 Número de publicación: **2 322 396**

⑤1 Int. Cl.:  
**H04L 12/58** (2006.01)

①2

## TRADUCCIÓN DE PATENTE EUROPEA

T3

⑨6 Número de solicitud europea: **06700722 .9**

⑨6 Fecha de presentación : **18.01.2006**

⑨7 Número de publicación de la solicitud: **1839417**

⑨7 Fecha de publicación de la solicitud: **03.10.2007**

⑤4 Título: **Sistema de seguridad para redes móviles.**

③0 Prioridad: **19.01.2005 US 644531 P**

④5 Fecha de publicación de la mención BOPI:  
**19.06.2009**

④5 Fecha de la publicación del folleto de la patente:  
**19.06.2009**

⑦3 Titular/es: **Markport Limited**  
**39/40 Upper Mount Street**  
**Dublin 2, IE**

⑦2 Inventor/es: **Nieuwenhuis, Taco**

⑦4 Agente: **Ungría López, Javier**

**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**

Sistema de seguridad para redes móviles.

5 **Campo de la invención**

La presente invención se refiere a un sistema de seguridad para redes móviles y un método de proporcionar mayor seguridad en redes móviles.

10 **Explicación de la técnica anterior**

Como sucede con el correo electrónico, los mensajes no solicitados o mensajes basura son un problema en el entorno de redes móviles. El contenido de estos mensajes tiene generalmente la finalidad de impulsar al receptor a utilizar algunos servicios cargados. Tales mensajes son una fuente de irritación para el usuario y a menudo son engañosos.

Como el correo electrónico basura, los mensajes basura son una fuente creciente de molestia para usuarios móviles. El contenido de estos mensajes tiene generalmente la finalidad de impulsar al receptor a usar algunos servicios tarifados, tal como llamar a un número 0800 de tarifa específica. Este fenómeno es irritante para el receptor no engañado, y también es engañoso cuando el usuario final que ha caído en la trampa, le eche la culpa eventualmente al operador. Usando direcciones fuente ficticias en sus mensajes, las partes de correo basura mantienen su identidad oculta a los operadores.

US2003/0083078 describe un nodo de enrutamiento con un módulo de discriminación de mensajes.

US6101393 describe un sistema para la aceptación selectiva de mensajes cortos.

La invención resuelve el problema de los mensajes no solicitados en redes móviles, en particular para lograr más flexibilidad a las técnicas usadas por las partes de envío de mensajes basura.

30 **Resumen de la invención**

Según la invención, se facilita un sistema de seguridad como el expuesto en la reivindicación 1.

35 La invención también proporciona un método como el expuesto en la reivindicación 11 implementado por un sistema de seguridad.

En una realización, el sistema bloquea mensajes que probablemente son no solicitados.

40 En otra realización, el sistema supervisa una dirección fuente de una petición de consulta y una dirección fuente de un mensaje correspondiente, y decide que es probable que el mensaje sea no solicitado si su dirección fuente es diferente de la de la petición de consulta correspondiente.

45 En una realización, el sistema guarda las peticiones de consulta solamente durante un período de tiempo preestablecido, y determina si una petición recibida dentro de dicho período de tiempo preestablecido se guarda en la memoria de datos cuando se busca en la memoria de datos a la recepción de un mensaje.

En otra realización, el sistema determina que una petición de consulta corresponde con un mensaje si tienen la misma dirección fuente.

50 En otra realización, el sistema activa el temporizador a la recepción de dicha petición.

En otra realización, el temporizador está configurado para funcionar desde el tiempo de recepción  $T_0$  hasta un límite de tiempo preestablecido  $T_{\text{preset\_end}}$ .

55 En otra realización, el sistema facilita el establecimiento del límite de tiempo del temporizador  $T_{\text{preset\_end}}$  para una categoría de petición de consulta.

**Descripción detallada de la invención**

60 **Breve descripción de los dibujos**

La invención se entenderá más claramente por la descripción siguiente de algunas de sus realizaciones, dadas a modo de ejemplo solamente con referencia a los dibujos acompañantes en los que:

65 La figura 1 es un diagrama de bloques que ilustra los componentes de un sistema de la invención.

La figura 2 es un diagrama de flujo que ilustra el flujo de datos a través del sistema de la figura 1.

Y las figuras 3 a 6 son diagramas de transferencia de mensajes que ilustran la operación del sistema con más detalle.

### Descripción de las realizaciones

Con referencia a la figura 1 una red móvil 1 incluye un sistema de seguridad 2 conectado a una puerta de enlace internacional de red móvil 3. La red móvil 1 incluye un HLR (registro de posición inicial) 10 y una pluralidad de dispositivos móviles de usuario 12. Las posiciones de los dispositivos 12 servidos por un operador se mantienen en el HLR 10. Para cada servicio terminado móvil pedido de la red, se precisa una petición de consulta o enviar información de enrutamiento (SRI) al HLR 10 para obtener información de posición con el fin de prestar satisfactoriamente el servicio, por ejemplo un mensaje posterior.

El sistema de seguridad 2 tiene un procesador 4 programado para supervisar peticiones SRI entrantes R1, R2 ... Rn y mensajes entrantes M1, M2 ... Mn. La configuración de enrutamiento dentro de la red móvil 1 es tal que todos los mensajes potencialmente sospechosos son dirigidos a través del sistema de seguridad 2 donde pueden ser analizados. Las peticiones SRI entrantes incluyen información de fuente. Los mensajes entrantes M1, M2 ... Mn están asociados con una petición SRI anterior. El sistema de seguridad 2 también incluye una memoria local de datos 5 y un reloj temporizador 6. Las peticiones SRI recibidas son supervisadas, la información de fuente asociada es copiada a la memoria local de datos 5 y se pone en marcha un contador asociado del reloj temporizador 6.

Algunas características típicas de los mensajes no solicitados o basura son las siguientes:

- El HLR es consultado por petición SRI una vez por MSISDN, independientemente de posibles servicios MT posteriores inmediatos, para hallar dónde puede residir típicamente un terminal móvil M1 de usuario final.
- La información de posición recuperada de la consulta HLR, en respuesta a una petición de consulta/petición SRI, es utilizada posteriormente en el período de tiempo T posterior para presentar mensajes no solicitados destinados al usuario final.
- El tráfico entra en una red mediante la puerta de enlace internacional y se dirige directamente al terminal móvil receptor M1 sin pasar por ningún centro de servicio local (y por lo tanto, deja a un lado los filtros de red locales).
- En los mensajes se utiliza una dirección fuente ficticia (para evitar el seguimiento del mensaje hasta la parte originante).
- Como resultado de la dirección fuente ficticia en el mensaje, el reconocimiento relacionado con el mensaje nunca llegará al verdadero originador. En contraposición a servicios MT de confianza regulares, el resultado de las entregas de mensajes individuales es irrelevante para el originador a condición de que tenga éxito un porcentaje significativo de entregas. Cabe esperar que el último criterio se cumpla debido a la petición SRI anterior que revela las posiciones típicas de las estaciones móviles M1, M2, ... Mn deseadas.

El sistema 1 y el método de la invención operan impidiendo el paso de mensajes con las características indicadas anteriormente. El método de operación implica supervisar peticiones SRI y mensajes entrantes. Como se ha indicado anteriormente, la información de posición recuperada de la consulta HLR, en respuesta a una petición de consulta/petición SRI, se usa entonces en el período de tiempo T posterior para presentar mensajes no solicitados destinados al usuario final. El reloj temporizador 6 se preestablece así para funcionar desde el tiempo de recepción de una petición SRI  $T_0$  hasta un límite de tiempo preestablecido  $T_{\text{preset\_end}}$ . El valor de temporizador se puede implementar en base a parámetros, tal como la posición de la fuente del SRI.

Con referencia a la figura 2, el método realizado por el sistema de seguridad 4 incluye los pasos siguientes:

1. Cuando entra en la red 1 una petición SRI a través de la puerta de enlace internacional 3:  
 Se pasa la petición,  
 Se pone en marcha un temporizador en el reloj 6,  
 Se copia información de fuente relevante a la memoria local de datos 5, incluyendo la dirección originante y la dirección de estación móvil terminante (MSISDN),  
 Si el temporizador expira sin un mensaje posterior, la información de fuente asociada de la petición SRI se quita de la memoria local o se mantiene internamente a efectos de seguimiento.
2. Un mensaje que entra en la red es supervisado y analizado y se actúa dependiendo del resultado del análisis.

## ES 2 322 396 T3

Si no se observó petición SRI anterior dentro de los límites de tiempo establecidos por el temporizador, no se pasa el mensaje y se genera un reconocimiento. Dado que es probable que la dirección fuente en el mensaje propiamente dicho sea ficticia, se espera que el reconocimiento no vuelva al verdadero originador y por lo tanto la opción entre un reconocimiento positivo o negativo es una opción dependiente de implementación del operador. El sistema asocia un mensaje con una petición de consulta en base a la identificación de estación móvil de terminación (MSISDN).

Si se observó una petición SRI anterior dentro del límite de tiempo anterior, se somete a otra prueba en la que la información de fuente del mensaje se compara con la información de fuente de la petición de posición anterior. Si las dos direcciones fuente no son idénticas, entonces no se pasa el mensaje. De nuevo, según entornos elegidos por el operador, se puede devolver un reconocimiento positivo o negativo. La dirección fuente de la petición SRI anterior puede ser marcada como sospechosa y mantenerse para investigación adicional cuando es la fuente verdadera de estos mensajes no solicitados.

Si las dos direcciones fuente concuerdan, se pasa el mensaje para entrega y se reinicia el temporizador.

Las figuras 3-6 ilustran la dinámica de operación del sistema con más detalle. El componente “@” se refiere a una entidad externa/fuente de mensajes, el componente “G” es la puerta de enlace a través de la que el mensaje/SRI entra en la red local, el componente “I” es el sistema de la invención, el componente “H” es el HLR local que contiene las posiciones de todos los dispositivos móviles en la red, y finalmente el pictograma móvil se refiere a los dispositivos móviles propiamente dichos.

La arquitectura (interna) del sistema de seguridad incluye un proxy que es capaz de ver los detalles relevantes de un mensaje pasante/petición SRI y una memoria de datos para mantener datos relevantes relacionados con peticiones SRI (recientes) de modo que estos detalles puedan ser comparados con los de mensajes posteriores.

En caso de que entre un SRI, se guarda al menos la información siguiente: dirección fuente del originador del SRI, identificación del móvil para el que se ha previsto la consulta, y la hora actual. Tan pronto como se recibe un mensaje propiamente dicho, se usa la dirección del receptor de dicho mensaje para realizar una consulta en la memoria. En caso de hallar un registro (o más) de una SRI anterior, la dirección fuente de dicho SRI se compara con la del mensaje propiamente dicho. Si no se halla ningún SRI anterior (figura 6), si no se halla ninguna dirección fuente concordante (figura 5) o si el tiempo entre el SRI y el mensaje propiamente dicho es mayor que algún valor configurable (figura 4), el mensaje no pasa. De otro modo, el mensaje es entregado normalmente (figura 3).

El sistema de la invención permite la supervisión y el control en tiempo real de mensajes no solicitados que llegan a una red móvil. Este método evita que los usuarios móviles reciban mensajes no rastreables con direcciones fuente ficticias de una fuente internacional supervisando y controlando el tráfico internacional como se ha descrito anteriormente.

El método de la invención sirve para evitar que mensajes no solicitados pasen a través de redes móviles. Tiene la ventaja de garantizar la rastreabilidad y de que los usuarios finales no sean molestados por estos mensajes.

La invención no se limita a las realizaciones descritas, sino que se puede variar en construcción y detalle.

## REIVINDICACIONES

1. Un sistema de seguridad para una red móvil (1) que tiene una puerta de enlace (3) para recibir mensajes de fuera de la red y un elemento de red (10) que guarda información de posición de terminal móvil, **caracterizado** porque el sistema de seguridad (2) está adaptado para:

supervisar en tiempo real peticiones de consulta que entran en la red a través de la puerta de enlace (3),

supervisar en tiempo real mensajes que entran en la red a través de la puerta de enlace y su correspondencia con dichas peticiones de consulta;

decidir según dicha supervisión si es probable que los mensajes sean no solicitados; y

donde el sistema incluye además una memoria de datos (5) y un temporizador (6), el sistema está adaptado para almacenar en la memoria de datos información con relación a peticiones de consulta recibidas de la puerta de enlace, y para decidir que es probable que un mensaje sea no solicitado si una petición de consulta anterior correspondiente no se ha recibido dentro de un período de tiempo preestablecido.

2. Un sistema según la reivindicación 1, donde el sistema está adaptado para determinar que una petición de consulta corresponde a un mensaje si tiene la misma dirección de terminación.

3. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para supervisar una dirección fuente de una petición de consulta y una dirección fuente de un mensaje correspondiente, y decide que es probable que el mensaje sea no solicitado si su dirección fuente es diferente de la de la petición de consulta correspondiente.

4. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para almacenar la información de petición de consulta en la memoria de datos (5) solamente durante un período de tiempo preestablecido, y determinar, cuando a la recepción de un mensaje se busca en la memoria de datos si se ha recibido una petición de consulta anterior correspondiente dentro de dicho período de tiempo preestablecido, si se guarda en la memoria de datos información con relación a dicha petición de consulta.

5. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para activar el temporizador a la recepción de una petición de consulta.

6. Un sistema según la reivindicación 5, donde el temporizador está configurado para funcionar desde el tiempo de recepción  $T_0$  hasta un límite de tiempo preestablecido  $T_{\text{preset\_end}}$ .

7. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para establecer el límite de tiempo del temporizador  $T_{\text{preset\_end}}$  para una categoría de petición de consulta.

8. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para bloquear mensajes que probablemente son no solicitados.

9. Un sistema según cualquier reivindicación precedente, donde el sistema es configurable para enviar un reconocimiento positivo o negativo según la supervisión.

10. Un sistema según cualquier reivindicación precedente, donde el sistema está adaptado para marcar como sospechosa y mantener para investigación adicional una dirección fuente de una petición de consulta correspondiente a un mensaje que probablemente es no solicitado.

11. Un método implementado por un sistema de seguridad (4) para supervisar mensajes en una red móvil que tiene una puerta de enlace (3) para recibir mensajes de fuera de la red y un elemento de red (10) que guarda información de posición de terminal móvil, **caracterizado** porque el método incluye los pasos del sistema de seguridad:

supervisar en tiempo real peticiones de consulta que entran en la red a través de la puerta de enlace (3);

supervisar en tiempo real mensajes que entran en la red a través de la puerta de enlace (3) y su correspondencia con dichas peticiones de consulta;

decidir según dicha supervisión si es probable que los mensajes sean no solicitados; y

donde el sistema (4) guarda en una memoria de datos (5) información con relación a peticiones de consulta recibidas de la puerta de enlace (3), y decide que es probable que un mensaje sea no solicitado si una petición de consulta anterior correspondiente no se ha recibido dentro de un período de tiempo preestablecido.

## ES 2 322 396 T3

12. Un método según la reivindicación 11, donde el sistema determina que una petición de consulta corresponde a un mensaje si tienen la misma dirección de terminación.

5 13. Un método según las reivindicaciones 11 o 12, donde el sistema supervisa una dirección fuente de una petición de consulta y una dirección fuente de un mensaje correspondiente, y decide que es probable que el mensaje sea no solicitado si su dirección fuente es diferente de la de la petición de consulta correspondiente.

10 14. Un método según cualquiera de las reivindicaciones 11 a 13, donde el sistema guarda la información de petición de consulta en la memoria de datos solamente durante un período de tiempo preestablecido, y determina, cuando se busca en la memoria de datos a la recepción de un mensaje si una petición de consulta anterior correspondiente ha sido recibida dentro de dicho período de tiempo preestablecido, si en la memoria de datos se guarda información con relación a tal petición de consulta.

15 15. Un método según cualquiera de las reivindicaciones 11 a 14, donde el sistema activa un temporizador (6) a la recepción de una petición de consulta.

16. Un método según la reivindicación 15, donde el temporizador funciona desde el tiempo de recepción  $T_0$  a un límite de tiempo preestablecido  $T_{\text{preset\_end}}$ .

20 17. Un método según cualquiera de las reivindicaciones 11 a 16, donde el límite de tiempo  $T_{\text{preset\_end}}$  se establece para una categoría de petición de consulta.

25 18. Un método según cualquiera de las reivindicaciones 11 a 17, donde el sistema bloquea mensajes que probablemente son no solicitados.

19. Un método según cualquiera de las reivindicaciones 11 a 18, incluyendo el paso adicional de enviar un reconocimiento positivo o negativo según la supervisión.

30 20. Un método según cualquiera de las reivindicaciones 11 a 19, donde el sistema (4) marca como sospechosa y mantiene para investigación adicional una dirección fuente de una petición de consulta correspondiente a un mensaje que probablemente es no solicitado.

35 21. Un medio legible por ordenador incluyendo código de software para realizar un método de cualquiera de las reivindicaciones 11 a 20 cuando se ejecuta en un procesador de datos digitales.

40

45

50

55

60

65

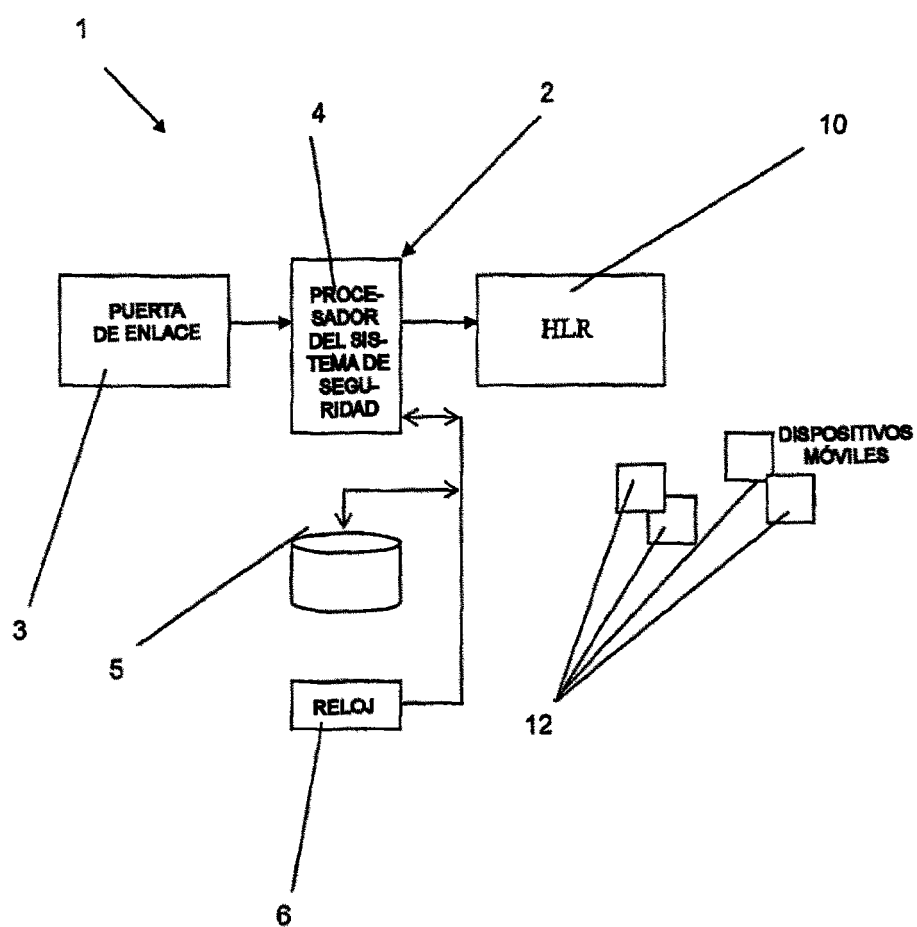


FIG. 1

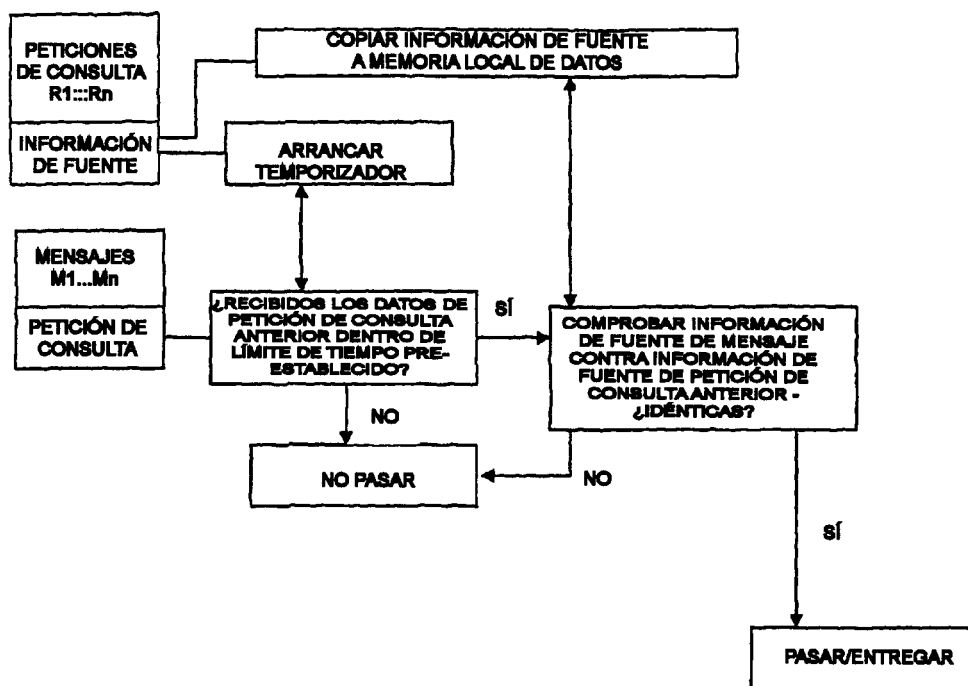
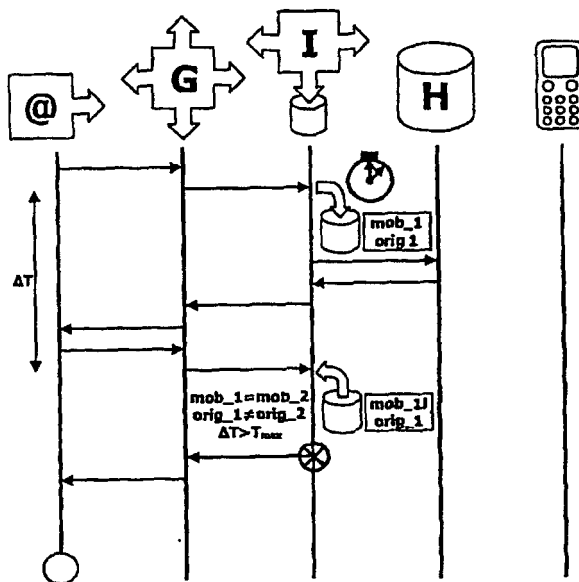


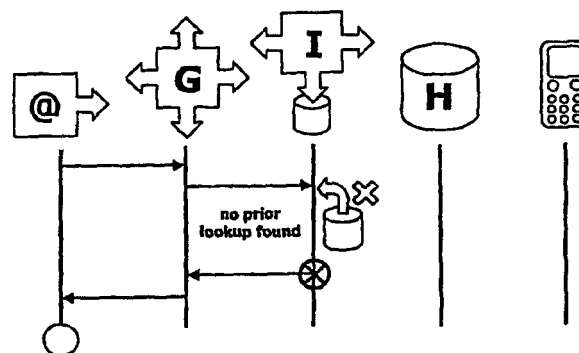
FIG. 2





**Escenario de mensajero no válido debido a una fuente de identificación no válida**

**Fig. 5**



**Escenario de mensajero no válido debido a no petición de consulta anterior**

**Fig. 6**