(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 274 956**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02700411 .8**
(86) Fecha de presentación : **25.01.2002**
(87) Número de publicación de la solicitud: **1358748**
(87) Fecha de publicación de la solicitud: **05.11.2003**

(54) Título: **Dispositivo y procedimiento de aparejamiento automático asegurado de los aparatos de una red de radiofrecuencia.**

(30) Prioridad: **26.01.2001 FR 01 01097**

(45) Fecha de publicación de la mención BOPI:
01.06.2007

(45) Fecha de la publicación del folleto de la patente:
01.06.2007

(73) Titular/es: **GEMPLUS**
avenue du Pic de Bertagne
Parc d'Activités de Gémenos
13881 Gémenos Cédex, FR

(72) Inventor/es: **Laporte, Frédéric;**
Hauser, Jean-Luc y
Rose, Murielle

(74) Agente: **Cañadell Isern, Roberto**

DESCRIPCIÓN

Dispositivo y procedimiento de aparejamiento automático asegurado de los aparatos de una red de radiofrecuencia.

El invento concierne las redes de radiofrecuencia en las que los aparatos de una red comunican entre sí mediante enlaces de radiofrecuencia y, más particularmente en dichas redes, un dispositivo y un procedimiento para aparejar entre sí de manera asegurada y automática los aparatos de la red.

Ya se sabe que se realizan enlaces de radiofrecuencia entre aparatos electrónicos, tales como un ordenador personal, una impresora, un combinado telefónico portátil o fijo, etc, poniendo en aplicación, por ejemplo, las especificaciones de una red denominada "BLUETOOTH" que se definen en los documentos ETS 300-328 y ETS 300-339.

En esta red BLUETOOTH, los aparatos comunican en "claro" de manera no asegurada o a través de mensajes codificados por algoritmos simétricos con clave privada.

Esta segunda solución permite una comunicación asegurada, pero entonces se plantea el problema del intercambio inicial de la clave. El estándar BLUETOOTH propone un intercambio en "claro" o la utilización de un cable para conectar ambos aparatos durante esta fase de intercambio de claves. Estas soluciones no son satisfactorias, ni sobre el plan práctico ni sobre el de la seguridad.

Para compensar este problema, se ha propuesto entrar manualmente la clave en cada uno de los dos aparatos que deben conectarse.

Este procedimiento puede resultar fastidioso en la medida en que se debe entrar dos veces dicho código en un teclado, este código puede tener numerosas cifras y/o letras.

Por otra parte, ciertos aparatos de la red puede que no tengan teclado, por ejemplo un auricular de un aparato portátil telefónico, de modo que nos veamos obligados a registrar este código continuamente o casi, en el aparato sin teclado. Esto permite que los portadores del aparato se introduzcan en la red sin tener que autentificarse en calidad de persona. También se propone conectar ambos aparatos por mediación de un enlace de cables, con objeto de intercambiar en toda seguridad las claves de sesión para asegurar seguidamente la autentificación y la codificación.

El inconveniente de esta solución radica en el hecho de que cada aparato debe estar equipado de un enchufe especial que será diferente en cada aparato.

En la solicitud de Patente Francesa Nº 2812509 depositada el 26 de julio de 2000 por la demandante, se propone un procedimiento de reconocimiento asegurado entre dos aparatos de una red de radiofrecuencia que comprende las siguientes etapas, las cuales consisten en:

(a) poner en marcha los dos aparatos,

(b) seleccionar uno de los dos aparatos como aparato-maestro y el otro como aparato-esclavo,

(c) acercar ambos aparatos a proximidad inmediata uno de otro,

(d) lanzar en el aparato-maestro un procedimiento automático de reconocimiento asegurado que consiste en:

- (d1) emitir señales según un diagrama de radiación, en el que las señales sólo las reciba el aparato-esclavo,
- (d2) lanzar un procedimiento clásico de conexión a la red de radiofrecuencia y, en caso de éxito, conexión a la red de radiofrecuencia,
- (d3) generar una clave de reconocimiento con vistas a asegurar los ulteriores intercambios
- (d4) emitir de nuevo señales según el diagrama de radiación habitual, y

(e) alejar los dos aparatos uno de otro para un funcionamiento a distancia normal.

Las etapas (d1) y (d2) se repiten si fracasa la etapa (d2) de conexión radiofrecuencia. Las etapas (d1) y (d2) se repiten por lo menos una vez, con un mayor diagrama de radiación de alcance.

El procedimiento que acabamos de describir es satisfactorio desde el punto de vista seguridad que éste proporciona, pero obliga a modificar los aparatos de la red para que su diagrama de radiación pueda modificarse, con el fin de que su alcance pueda reducirse a unos centímetros durante su reconocimiento mutuo.

El documento EP-A-1024626 describe un procedimiento y un dispositivo que permite que actúen entre sí dos aparatos de radiofrecuencia.

Un objetivo del presente invento consiste en realizar un dispositivo dedicado al aparejamiento asegurado de los aparatos de una red de radiofrecuencia sin que sea necesario modificar los aparatos de la red de radiofrecuencia.

Por otra parte, los procedimientos del arte anterior implican, por parte del usuario de los aparatos de radiofrecuencia, el conocimiento de los códigos y la manipulación de teclas en los aparatos para entrar dichos códigos y, eventualmente, la manipulación de cables de conexión entre ambos aparatos que deben conectarse. Otra finalidad del presente invento consiste en realizar un dispositivo dedicado al aparejamiento asegurado de los aparatos de una red de radiofrecuencia, que permita el aparejamiento automático de cada aparato de la red de radiofrecuencia a medida de las necesidades de conexión.

El invento concierne, así pues, un dispositivo de aparejamiento asegurado y automático de los aparatos de una red de informática, caracterizado por comprender:

- un módulo de conexión para comunicar con cada uno de los aparatos de dicha red de radiofrecuencia, y

- un módulo electrónico de aparejamiento que permite suministrar a un aparato de la red una clave de aparejamiento para comunicar, por lo menos, con otro aparato de la red de radiofrecuencia.

El módulo de conexión comprende medios para limitar el alcance de emisión/recepción del dispositivo y el módulo electrónico de aparejamiento comprende:

- como mínimo una memoria para registrar un código o clave de cifrado en los aparatos que deben aparejarse,

- un circuito de mando de la memoria para realizar un procedimiento automático de conexión y suministrar a un aparato de la red una clave de aparejamiento.

El dispositivo según el invento puede comprender, además, una interfaz Hombre/Máquina que comprende por lo menos una tecla de mando Marcha/Parada.

Esta interfaz puede comprender, además, una pantalla de visualización para visualizar, principalmente, informaciones de funcionamiento del dispositivo.

La memoria puede estar prevista para registrar las distintas claves de aparejamiento en los aparatos que deben aparejarse.

Las claves de aparejamiento puede suministrarlas un generador de claves.

El invento concierne igualmente un procedimiento de aparejamiento asegurado y automático de los aparatos de una red de radiofrecuencia por mediación del dispositivo descrito anteriormente, caracterizado por comprender las siguientes etapas que consisten en:

(a) acercar el dispositivo a proximidad inmediata (unos centímetros) del aparato que debe aparejarse,

(b) activar el dispositivo y el aparato que deben aparejarse,

(c) suministrar al aparato que debe aparejarse por lo menos una clave de aparejamiento para que pueda utilizarse, por lo menos, durante las comunicaciones con otro aparato de la red, y

(d) volver a la etapa (a) para aparejar otro aparato.

Otras características y ventajas del presente invento aparecerán cuando se lea la siguiente descripción de un ejemplo particular de realización, dicha descripción se hace en relación con los dibujos adjuntos en los que:

- la figura 1 muestra esquemáticamente una red de radiofrecuencia que conecta varios aparatos entre sí, y

- la figura 2 es un esquema funcional simplificado de un dispositivo según el invento,

El invento que describimos se aplica a una red de radiofrecuencia 80 (figura 1) realizada y funcionando según las especificidades del sistema descrito anteriormente BLUETOOTH. Esta red 60 está prevista, por ejemplo, para conectar un aparato telefónico portátil 10 a un auricular 12 y a un ordenador personal 26, éste último está conectado vía la red 60 a un teclado 32.

Con este fin, los distintos aparatos 10, 12, 26 y 32, están equipados de un módulo BLUETOOTH 50 que emite y recibe señales radioeléctricas, vía una antena 14 para el aparato telefónico portátil, 16 para el auricular, 52 para el ordenador personal, 26 y 54 para el teclado 32.

En el estado actual del sistema BLUETOOTH, la conexión de un aparato a la red debe efectuarse según un proceso particular que implica manipulaciones por parte del usuario del aparato concernido, por ejemplo, entrar un código de

acceso con las teclas 56 del teclado 32, o las teclas 20 del aparato telefónico portátil 10. También pueden utilizarse otras teclas de Marcha/Parada 24 y de "navegación" 22 en una pantalla 18.

Si no hubiera estas teclas en el aparato que debe conectarse, se han previsto conexiones por cable, por ejemplo para aparejar el auricular 12 al aparato telefónico portátil 10 o para aparejar el teclado 32 al ordenador personal 26.

Durante el proceso de conexión o de aparejamiento a la red es cuando los aparatos, susceptibles de comunicar entre sí, intercambian claves de reconocimiento o de aparejamiento, las cuales se utilizan seguidamente para efectuar ulteriormente comunicaciones de manera asegurada.

En la solicitud de la patente anteriormente citada, se ha descrito un procedimiento para asegurar este proceso de conexión o de aparejamiento entre dos aparatos de la red, por ejemplo entre el auricular 12 y el aparato telefónico portátil 10.

El invento propone un dispositivo para aparejar de manera automática y asegurada cada aparato a la red, de tal modo que cada aparato pueda conectarse seguidamente a otro, o a varios aparatos de la red.

Según el invento, este dispositivo puede presentarse en forma de una tarjeta con chip electrónico sin contacto 34 o bajo cualquier otra forma.

Cualquiera que sea su forma exterior, este dispositivo comprende esencialmente (figura 1 y 2):

- un módulo BLUETOOTH 50 asociado a una antena 38, que comprende esencialmente medios de emisión/recepción, que funcionan según las especificaciones de las normas citadas anteriormente, y

- un módulo electrónico de aparejamiento 60.

El módulo BLUETOOTH puede reemplazarse por un módulo de comunicación a distancia equivalente, tales como los que funcionan por haz de infrarrojos, por aparejamiento magnético o capacitivo.

También puede comprender:

- una interfaz hombre/máquina 70 que puede o no incluir:

  - una o varias teclas de mando 2,

  - y/o una pantalla de visualización 74.

El módulo electrónico de aparejamiento 60 comprende:

- Una memoria 62 para registrar por lo menos un código o una clave de aparejamiento,

- Un circuito de mando 66 que suministra señales de mando de la memoria 62 y del módulo BLUETOOTH 50.

En presencia de la interfaz hombre/máquina 70, el circuito de mando recibe señales de las teclas 72 y suministra señales de visualización para la visualización en la pantalla 74.

La memoria 62 puede reemplazarse o completarse por un generador de claves 64.

El módulo electrónico de aparejamiento 60 se realiza de preferencia con un microcontrolador y sus memorias asociadas sirven de programas específicos, principalmente para efectuar cálculos criptográficos y controlar el proceso de aparejamiento.

El módulo BLUETOOTH y, más particularmente, los medios de emisión/recepción están calibrados para tener un diagrama de radiación cuyo alcance sólo es de unos centímetros.

Si el dispositivo según el invento es de tipo sin contacto, se le deberá suministrar la energía eléctrica para su funcionamiento, ya sea mediante una pila eléctrica, ya sea mediante la energía de alta frecuencia recibida del aparato que debe aparejarse por mediación de un circuito de retrocesión y filtrado de tipo clásico.

El dispositivo según el invento debe aplicarse según las siguientes etapas que consisten en:

(a) acercar el dispositivo 40 a proximidad inmediata (unos centímetros) del aparato que debe aparejarse 10, 12, 26 o 32.

(b) activar el dispositivo 40 y el aparato que debe aparejarse 10, 12, 26 o 32,

(c) suministrar al aparato que debe aparejarse 10, 12, 26 o 32 por lo menos una clave de aparejamiento para poder utilizarla durante las comunicaciones con otro aparato de la red, y

(d) volver a la etapa (a) para aparejar otro aparato.

El procedimiento de reconocimiento entre el dispositivo 40 y el aparato que debe aparejarse consiste esencialmente en comparar claves suministradas por el dispositivo 40 y el aparato que debe aparejarse y en determinar que estén autorizados a comunicar entre sí en caso de comparación positiva.

Las claves que deben compararse pueden estar contenidas en la memoria 62 del dispositivo o en una memoria semejante del aparato que debe aparejarse; también pueden calcularse gracias al generador de claves 64 o a un circuito de cálculo semejante al aparato que debe aparejarse.

Estas claves de aparejamiento, las cuales permiten reconocer que el aparato que debe aparejarse está autorizado a ser conectado a la red de radiofrecuencia del usuario del dispositivo 40, son diferentes a la clave que se utiliza para asegurar las comunicaciones entre los aparatos que deben aparejarse (etapa (d)). Las etapas (a) y (b) las efectúa el usuario del dispositivo 40, mientras que las etapas (c) y (d) las efectúa el dispositivo 40 con el mando del circuito 66.

La interfaz Hombre/Máquina 70 permite al usuario, mediante las teclas 72, ser el iniciador de ciertas etapas, tales como las etapas (a) y (b) o estar informado por la pantalla 74, sobre las etapas efectuadas, o en curso, o sobre la identidad del aparato que debe aparejarse, en curso de aparejamiento o ya aparejado.

Sin embargo, esta interfaz Hombre/Máquina puede reducirse a una sola tecla de mando para activar el dispositivo 40 (etapa b), las siguientes etapas las efectúa automáticamente el dispositivo 40. El dispositivo 40 está previsto para inicializar todos los aparatos que el usuario es susceptible de utilizar en la red de radiofrecuencia y, por ello, dispone en la memoria 62 del usuario de las claves de aparejamiento asignadas a cada aparato que debe aparejarse.

De este modo, la memoria 62 puede contener, además de las claves de aparejamiento, parámetros de configuración del aparato que debe aparejarse, los cuales se le transmitirán en el momento de su lanzamiento inicial después de que se le haya entregado al usuario. Estos parámetros o algunos de ellos, también pueden retransmitirse al aparato que debe aparejarse, cada vez que se pone en red, según el procedimiento del invento.

El dispositivo según el invento comprende de preferencia un juego de claves para permitir distintos aparejamientos o un generador de claves. Este dispositivo puede comprender, asimismo, medios de accionamiento para cambiar las claves que deben compartir los distintos aparatos, tales como teclas, teclados u otros.

El dispositivo realiza un almacenamiento de claves. En el momento de su utilización, se acercará a los aparatos que deben comunicar juntos para suministrarles una clave común.

El dispositivo también comprende medios 66 para administrar las distintas claves, principalmente para asignarlas a cada aparato, ya sea cuando interviene el usuario con el teclado, ya sea automáticamente asociándolo al identificarte del aparato.

Durante la transmisión de la clave, el dispositivo puede recibir del aparato sus características, las cuales se memorizan asociándolas a un identificante de la clave para permitir administrar las claves.

El dispositivo y el procedimiento según el invento presentan las siguientes ventajas:

- el aparato que debe aparejarse no necesita ninguna adaptación particular, tal como un lector de tarjeta con chip, cables de conexión, o una tecla de mando particular para poder conectarse a la red;

- el usuario del dispositivo no necesita conocer uno o varios códigos de acceso, puesto que ya están contenidos en la memoria 62;

- el aparato que debe aparejarse está configurado según ciertas características registradas en la memoria 62, es decir sin intervención del usuario, excepto si éste desea modificarlas;

- las informaciones y parámetros personales del usuario se registran en la memoria 62 y están protegidos contra todo tipo de fraude;

- el aparejamiento se efectúa de manera automática y asegurada con una intervención mínima por parte del usuario.

REIVINDICACIONES

1. Dispositivo de aparejamiento automático y asegurado (40) de los aparatos de una red de radiofrecuencia, que comprenden:

- un módulo de conexión (50,38) para comunicar con cada uno de los aparatos de dicha red de radiofrecuencia, y

- un módulo electrónico de aparejamiento (60) que permite suministrar a un aparato de la red (10, 12, 26 o 32) una clave de aparejamiento para comunicar, por lo menos, con otro aparato de la red de radiofrecuencia,

caracterizado porque dicho módulo de conexión comprende medios para limitar el alcance de emisión/recepción del dispositivo y porque dicho módulo electrónico de aparejamiento comprende:

- Como mínimo una memoria (62) para registrar un código o clave de cifrado en los aparatos que deben aparejarse,

- Un circuito de mando (66) de la memoria (62) para realizar un procedimiento automático de conexión y suministrar a un aparato de la red una clave de aparejamiento.

2. Dispositivo según la reivindicación 2, **caracterizado** porque el módulo de conexión (50,38) es del tipo radiofrecuencia, permitiéndole conectarse a dicha red de radiofrecuencia.

3. Dispositivo según la reivindicación 1 o 2, **caracterizado** porque comprende además una interfaz Hombre/Máquina (70) que comprende por lo menos una tecla de mando (72) de Marcha/Parada del dicho dispositivo.

4. Dispositivo según la reivindicación 3, **caracterizado** porque la interfaz Hombre/Máquina (70) comprende, además, una pantalla de visualización (74).

5. Dispositivo según una de las reivindicaciones de 1 a 4, **caracterizado** porque la memoria (62) está prevista para registrar las distintas claves de aparejamiento en los aparatos que deben aparejarse.

6. Dispositivo según una de las reivindicaciones de 1 a 5, **caracterizado** porque la memoria (62) está prevista para registrar las distintas características del aparato receptor de una clave de aparejamiento.

7. Dispositivo según una de las reivindicaciones de 1 a 6, **caracterizado** porque la memoria (62) está prevista para registrar las distintas configuraciones de los aparatos susceptibles de ser aparejados por dicho dispositivo.

8. Dispositivo según una de las reivindicaciones de 1 a 7, **caracterizado** porque la clave de cifrado la facilita un generador de claves de cifrado.

9. Dispositivo según una de las reivindicaciones de 1 a 8, **caracterizado** porque comprende medios (64, 66) para cambiar las claves de aparejamiento de los aparatos.

10. Dispositivo según una de las reivindicaciones de 1 a 9, **caracterizado** porque comprende medios (66) para administrar la asignación de las claves a los distintos aparatos.

11. Objeto portátil que contiene un dispositivo según cualquiera de las reivindicaciones de 1 a 10, **caracterizado** porque se presenta en forma de una tarjeta con chip electrónico.

12. Procedimiento de aparejamiento automático y asegurado, de los aparatos de una red de radiofrecuencia por mediación de un dispositivo u objeto según una de las reivindicaciones anteriores de 1 a 11, **caracterizado** porque comprende las siguientes etapas que consisten en:

(a) acercar el dispositivo (40) a proximidad inmediata (unos centímetros) del aparato que debe aparejarse (10, 12, 26 o 32),

(b) activar el dispositivo (40) y el aparato que deben aparejarse (10, 12, 26 o 32),

(c) suministrar al aparato que debe aparejarse (10, 12, 26 o 32), por lo menos una clave de aparejamiento para que pueda utilizarse, por lo menos, durante las comunicaciones con otro aparato de la red, y

(d) volver a la etapa (a) para aparejar otro aparato.

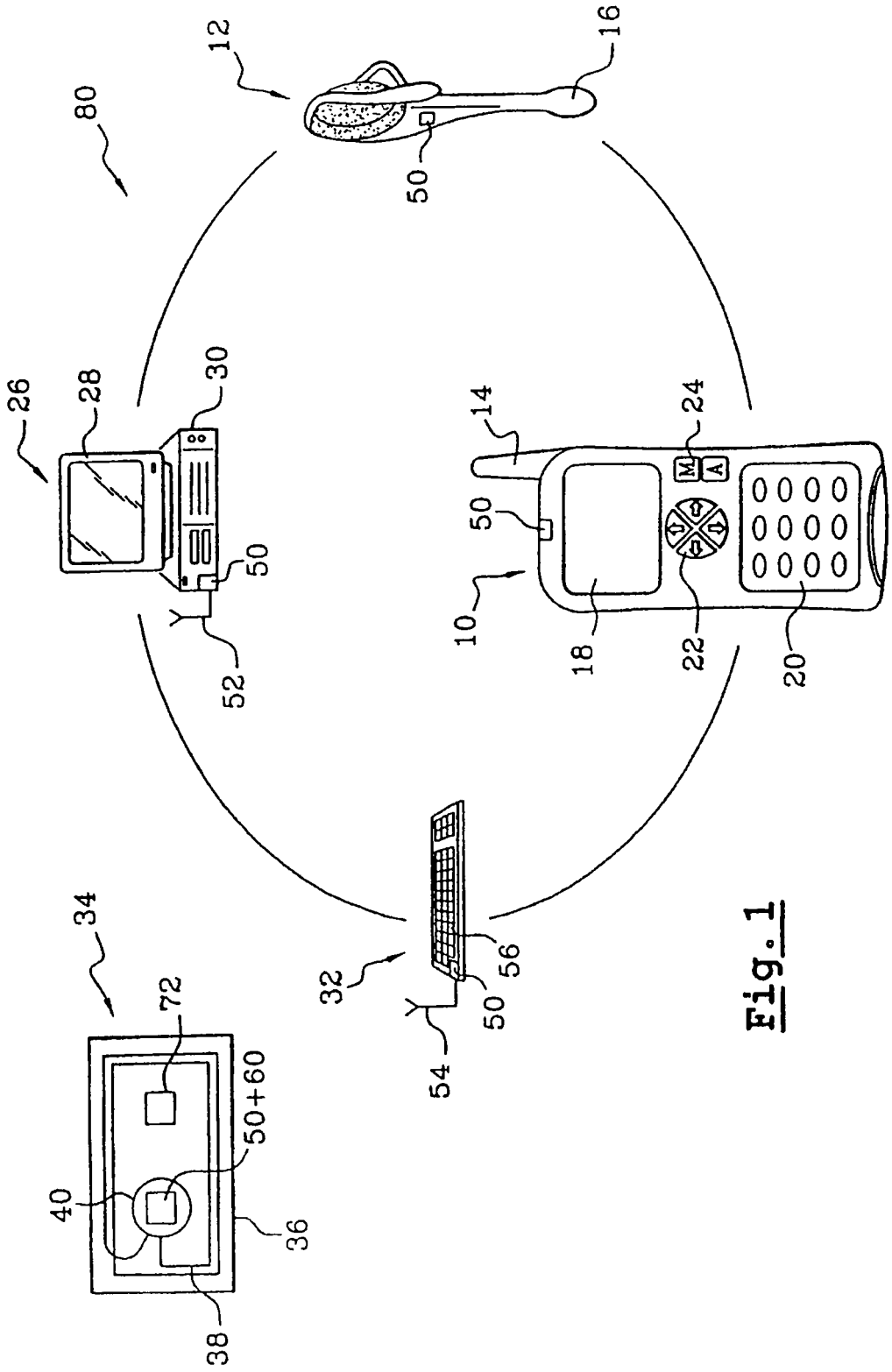
80
12
16
50
26
28
30
50
52
14
24
50
10
18
22
20
34
72
50+60
40
36
38
32
50
56
54

Fig. 1

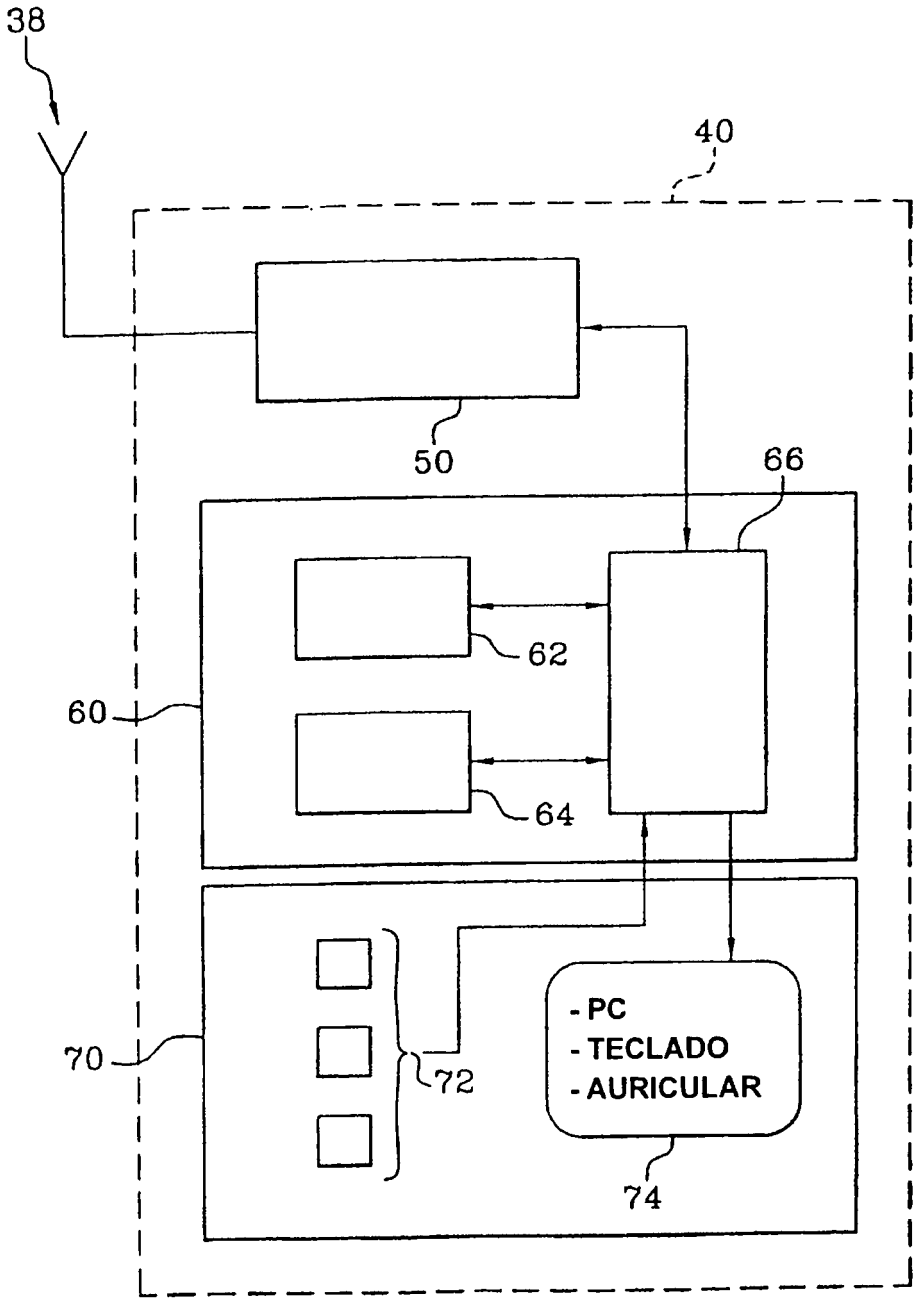

Fig. 2