

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 952 840**

51 Int. Cl.:

G08B 29/04 (2006.01)

H04K 3/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **15.03.2018** **E 18161928 (9)**

97 Fecha y número de publicación de la concesión europea: **02.08.2023** **EP 3540707**

54 Título: **Un método y un dispositivo de detección de perturbaciones radioeléctricas en un sistema de radiocomunicaciones**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
06.11.2023

73 Titular/es:

VERISURE SÀRL (100.0%)
Chemin Jean-Baptiste Vandelle 3/3A
1290 Versoix, CH

72 Inventor/es:

SKARP, FILIP

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 952 840 T3

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

DESCRIPCIÓN

Un método y un dispositivo de detección de perturbaciones radioeléctricas en un sistema de radiocomunicaciones

Campo técnico

La invención se refiere a un método y un dispositivo de detección de perturbaciones radioeléctricas en un sistema de radiocomunicaciones.

Técnica anterior

En el documento EP2541518 se da a conocer un sistema de alarma de la técnica anterior para gestionar situaciones de interferencia forzada [*jamming*]. Una primera instalación de alarma está dispuesta para supervisar una segunda instalación de alarma y para monitorizar señales de radiocomunicaciones intercambiadas en dicha segunda instalación de alarma. La ausencia de señales de radiocomunicaciones monitorizadas dará como resultado la generación de una señal de alarma de interferencia forzada. Cabe señalar que si la comunicación entre un dispositivo periférico y una pasarela en cualquiera de las instalaciones de alarma se interrumpe durante un período de tiempo más largo, como varios minutos, se puede generar una alarma de supervisión en esa instalación de alarma. El documento US2004203423 sugiere un método para detectar intentos de interferencia forzada en ráfagas de datos. Se determina un nivel de potencia de las ráfagas y a continuación se verifica si una ráfaga ha sido identificada como aceptable ("modulada") o inaceptable ("no modulada"). A continuación se verifica si el RSSI de las ráfagas no moduladas está por encima de un umbral o por debajo de un umbral. Si está por encima, se activa una bandera.

Compendio de la invención

De acuerdo con un primer aspecto, se proporciona un método de detección de perturbaciones radioeléctricas en un sistema de radiocomunicaciones que comprende un dispositivo de pasarela y un dispositivo periférico, cada uno dispuesto para enviar señales de radiocomunicaciones hacia y para recibir señales de radiocomunicaciones del otro. El método se define en la reivindicación 1. En la reivindicación 10 se define un detector correspondiente.

Como resultado, se pueden detectar métodos de interferencia forzada más sofisticados y se puede configurar una alarma de interferencia forzada, en caso de que se realicen intentos de interferencia forzada. Una alarma de interferencia forzada puede comprender la generación de una señal de alarma en instalaciones en las que está instalado el sistema de radiocomunicaciones y/o el reenvío de una señal de alarma a una estación de monitorización central remota donde se pueden tomar medidas adicionales para gestionar la situación. El método proporcionará una mayor seguridad en la detección de intentos sofisticados de interferencia forzada dirigida en sistemas de radiocomunicaciones en general y en sistemas de alarma en particular, incluso cuando una señal de interferencia forzada altere o destruya segmentos de información específicos intercambiados en la radiocomunicación.

El método dado a conocer se puede utilizar en un sistema doméstico de comunicaciones inalámbricas que comprende una pluralidad de nodos inalámbricos que incluyen una primera pasarela, al menos un dispositivo periférico inalámbrico y, en algunas instalaciones, al menos una segunda pasarela. El sistema de comunicaciones inalámbrico doméstico forma una instalación que puede incluir un sistema de seguridad doméstico convencional que comprende al menos un detector de alarma inalámbrico y al menos una pasarela. Si alguno de los dispositivos o nodos falla, se toman algunas medidas, como informar al propietario de la casa o activar una alarma de manipulación. La alarma de manipulación puede comprender la generación de una señal de alarma en instalaciones en las que está instalado el sistema de radiocomunicaciones y/o el reenvío de una señal de alarma a una estación de monitorización central remota donde se pueden tomar medidas adicionales para gestionar la situación.

Un sistema de comunicaciones inalámbrico doméstico en general puede ser cualquier tipo de sistema inalámbrico que comprenda una pluralidad de nodos inalámbricos periféricos, como una alarma de intrusión y una unidad central. En concreto, puede ser un sistema de seguridad que disponga de una pluralidad de detectores inalámbricos, sensibles a la presencia o paso de personas y objetos, que se comunican con una unidad central tal como una pasarela mediante comunicación inalámbrica.

Las interferencias o medidas de perturbaciones radioeléctricas intencionadas pueden ser causadas por un bloqueador [*jammer*] de radiocomunicaciones que es un dispositivo que, de manera deliberada, bloquea, interfiere con o interfiere forzosamente con comunicaciones inalámbricas autorizadas. En algunos casos, los bloqueadores funcionan mediante la transmisión de señales de radiocomunicaciones que interrumpen las comunicaciones al reducir la relación señal/ruido. El concepto se puede utilizar en redes de datos inalámbricas para interrumpir el flujo de información. La interferencia forzada generalmente se distingue de la interferencia que puede producirse debido al mal funcionamiento del dispositivo u otras circunstancias accidentales. Existen algunos tipos de 'interferencias forzadas' no intencionadas. Una forma de ellas se produce cuando un operador transmite en una frecuencia ocupada sin verificar primero si la misma está siendo utilizada o sin poder recibir señales de estaciones que usan la frecuencia. Otra forma de interferencia forzada no intencionada se produce cuando el equipo radia accidentalmente una señal de una frecuencia que alterará la comunicación que usa esa frecuencia.

Una de las aplicaciones de los sistemas de comunicaciones inalámbricos domésticos es los sistemas de alarma. Los sistemas de seguridad y alarma utilizados hoy en día normalmente comprenden un panel de control y una pasarela que está conectada a una estación central, ya sea por una línea telefónica o por un sistema de telecomunicaciones inalámbricas, tal como el GSM u otros sistemas de radiofrecuencia. La conexión también puede ser a través de internet. El panel de control puede estar provisto de un dispositivo de entrada o ser activado y controlado por un dispositivo de control tal como un teclado el cual puede ser un dispositivo remoto inalámbrico.

En los sistemas de comunicación digital que utilizan paquetes, los métodos de interferencia forzada sofisticados incluyen el *sniping* de paquetes que destruirá la comunicación entre las pasarelas y los dispositivos periféricos sin aumentar el ruido de fondo continuamente. Un bloqueador de *sniping* de paquetes normalmente incorporaría una cadena de recepción inteligente y se situaría a la escucha de paquetes o energía transmitidos por vía aérea durante la comunicación inalámbrica digital. En este contexto, un paquete comprende un conjunto de datos de preámbulo, palabra de sincronización, carga útil y verificación de redundancia cíclica (CRC). Una vez que se detecta el inicio de un paquete, el bloqueador puede emitir un breve pico de potencia que dura solo una fracción de la longitud del paquete (la longitud real se basaría en el protocolo en el que se aplica la interferencia forzada, si, por ejemplo, se usa una codificación de corrección de errores, se debería aplicar la interferencia forzada a más bits para garantizar un paquete destruido). Esto destruiría uno o una pluralidad de bits en alguna parte del paquete haciendo que el paquete, por ejemplo, sea ignorado debido a la destrucción de la palabra de sincronización, se llene con un contenido completamente sin sentido o no supere la verificación de redundancia cíclica (CRC).

En varias realizaciones, la potencia de la señal entrante se mide continuamente y en un detector se detectan cambios en esa potencia. Al medir la energía por bit del flujo continuo de bits recibido, es posible detectar cambios escalonados, tanto positivos como negativos, que surgirían por el *sniping* de paquetes. La medición continua de la potencia podría realizarse en cualquier posición adecuada en la cadena de recepción. La medición se realiza con un ancho de banda suficientemente alto (la velocidad de medición de la potencia debe ser del orden de la tasa de bits de la señal recibida). Dependiendo de la arquitectura del receptor, las mediciones de potencia se pueden realizar midiendo la potencia de la señal entrante en partes relevantes del receptor de radiocomunicaciones, tales como el Control de Ganancia Automatizado (AGC), el Amplificador de Frecuencia Intermedia (IF AMP) o el Convertidor analógico a digital (ADC). La medición de potencia también se puede realizar midiendo el nivel de los datos de IQ digitales. En la práctica, se utilizan diferentes métodos de medición según la arquitectura del receptor.

Breve descripción de los dibujos

A continuación se describirán realizaciones no limitativas de la invención con referencia a las figuras en las que:

La Fig. 1 es una vista esquemática de una instalación de un sistema inalámbrico doméstico,

La Fig. 2 es un diagrama esquemático que muestra la potencia de una señal de radiocomunicaciones recibida en una situación de interferencia forzada simple en el dominio del tiempo,

La Fig. 3 es un diagrama esquemático que muestra la potencia de una señal de radiocomunicaciones recibida en el dominio del tiempo donde un bloqueador de *sniping* genera una señal de interferencia forzada de una manera más sofisticada,

La Fig. 4 muestra esquemáticamente mediciones de señal correspondientes a la señal que se muestra en la Fig. 3,

La Fig. 5 es un diagrama esquemático que muestra un receptor de tipo analógico que comprende una realización de un detector de acuerdo con la invención,

La Fig. 6 es un diagrama esquemático que muestra un receptor de tipo digital que comprende una realización de un detector de acuerdo con la invención,

La Fig. 7 es un diagrama esquemático que muestra una realización de un detector de acuerdo con la invención,

La Fig. 8 es un diagrama esquemático que muestra una instalación típica que incluye dos unidades de comunicación que comprenden un detector de acuerdo con la invención,

La Fig. 9 es una tabla que muestra parte de un paquete de un flujo continuo de bits recibido correctamente y los niveles de energía correspondientes, y

La Fig. 10 es una tabla que muestra parte de un paquete recibido de un flujo continuo de bits sometido a interferencia forzada y los niveles de energía correspondientes.

Descripción detallada

La Fig. 1 muestra un sistema inalámbrico doméstico instalado en un edificio 10. El sistema inalámbrico doméstico es una instalación de sistema de alarma y comprende una pluralidad de nodos periféricos inalámbricos que incluyen dispositivos periféricos inalámbricos, una primera pasarela 12 y una segunda pasarela 12'. La segunda pasarela 12' está alimentada por la red y normalmente no está provista de una batería de respaldo. Un nodo periférico inalámbrico

es un primer detector 14 de infrarrojos montado en la esquina de una sala cerca del techo. El primer detector 14 de infrarrojos tiene un área de detección que cubre la primera pasarela 12. Un primer detector 16 de alarma perimetral está montado en una ventana 17 en la misma sala. El detector de infrarrojos funciona de manera convencional para detectar la presencia y movimientos de objetos que emiten radiación infrarroja. El detector de alarma perimetral también funciona de manera convencional para detectar el momento en el que se abre una puerta o una ventana. En varias realizaciones, el detector de alarma perimetral comprende un sensor magnético que detectará el momento en el que se mueva un imán fijado a la puerta o ventana.

La segunda pasarela 12' está dispuesta en una segunda sala separada de la sala donde está dispuesta la primera pasarela 12. Un segundo detector 14' de infrarrojos está montado en la misma sala que la segunda pasarela 12' para cubrirla dentro de su área operativa y un segundo detector 16' de alarma perimetral está montado en una segunda ventana 17' en la misma sala. Un teclado 19 está montado cerca de una puerta delantera 20 del edificio 10. El teclado 19 es utilizado por un operador del sistema de alarma para armar y desarmar el sistema de alarma. El teclado 19 también es un nodo periférico inalámbrico. La puerta delantera 20 está cubierta por un tercer detector 21 de alarma perimetral. Otro tipo de dispositivo periférico inalámbrico es un detector 23 de humo montado en el techo del edificio. En varias realizaciones, una pluralidad de detectores 23 de humo están dispuestos por todo el edificio 10 para garantizar que el incendio pueda detectarse en una etapa temprana.

Dependiendo de diferentes circunstancias, la primera pasarela 12 y la segunda pasarela 12' se conectan a una estación 22 de monitorización central remota bien a través de una conexión 24 por cable o bien a través de una conexión inalámbrica tal como el GSM o una red celular digital similar 34. La conexión con la estación 22 de monitorización central remota también puede ser a través de internet 26. En la realización que se muestra en la Fig. 1, la conexión de internet se proporciona a través de un enrutador inalámbrico 32 que está conectado a Internet por fibra, cable o una Línea de Abonado Digital, tal como ADSL. En la realización que se muestra en la Fig. 1, la segunda pasarela 12' está conectada por cable 33 al enrutador inalámbrico 32. La conexión 24 por cable puede ser parte de una red telefónica pública conmutada 25. En varias realizaciones, la estación 22 de monitorización central remota comprende un módulo 27 de interfaz, una base 28 de datos y un servidor *web* 29. La base 28 de datos almacena datos de instalación y aplicación relacionados con la instalación, incluidos todos los nodos de la red inalámbrica y ajustes de la alarma.

La primera pasarela 12 es capaz de comunicarse con la segunda pasarela 12' gracias a las unidades de transmisión de radiocomunicaciones más potentes, aunque algunos nodos periféricos no pueden hacerlo. Al colocar pasarelas estratégicamente dentro de un edificio, es posible garantizar que cada nodo periférico tenga un enlace de RF adecuado con al menos una pasarela. Siempre que cada pasarela pueda comunicarse directamente con al menos otra pasarela y directa o indirectamente con todas las demás pasarelas, la instalación funcionará correctamente. Para lograr una redundancia completa, la instalación debe incluir suficientes pasarelas para que cada nodo periférico pueda comunicarse con al menos dos pasarelas.

Una instalación tal como el sistema de alarma que se muestra en la Fig. 1 contiene una gran cantidad de información de estados dinámica, tal como estado de armado, estado de alarma, estado de batería periférica, etc. en un conjunto de datos de información de estado del sistema total. También se almacena información similar en otros tipos de sistemas inalámbricos domésticos. Cada pasarela o controlador recibe continuamente entradas de diferentes fuentes autenticadas, como nodos periféricos, una estación de monitorización central remota (RCMS), sistemas adyacentes, etc. que afecta a un estado distribuido de la aplicación o sistema.

En varias realizaciones, una segunda pasarela puede utilizar el enlace de comunicación de RF de otra pasarela para tunelizar mensajes a una RCMS. Por ejemplo, si el enlace ascendente de la segunda pasarela a la RCMS es muy lento o inalcanzable, o tiene un coste mayor, se puede utilizar el enlace ascendente de otra pasarela.

El diagrama esquemático de la Fig. 2 muestra niveles de potencia de señales de radiocomunicaciones recibidas en una situación de interferencia forzada en el dominio del tiempo en el que una señal 40 de interferencia forzada se transmite como ruido. Las señales 42 de mensaje recibidas con un nivel de potencia PA se ocultan o al menos no se pueden leer completamente cuando un nivel de ruido PN se extiende por encima del nivel PA de las señales de mensaje. Cuando se detecta una situación de interferencia forzada como la que se muestra en la Fig. 2 en sistemas de la técnica anterior, se puede generar una alarma de interferencia forzada.

El diagrama esquemático de la Fig. 3 muestra una situación de interferencia forzada en el dominio del tiempo en la que un bloqueador de *sniping* genera una señal de interferencia forzada de una manera más sofisticada. Un bloqueador de *sniping* normalmente comprende una cadena de recepción más inteligente y se situará a la escucha de señales 42 de mensaje o energía transmitidas por vía aérea. Una vez que se detecta una señal 42 de mensaje, tal como un paquete, el bloqueador emite un breve pico 43 de potencia con el nivel de potencia PN que dura al menos, y normalmente solo, una fracción de la longitud del paquete. La longitud real normalmente se basaría en el protocolo en el que se aplica la interferencia forzada. Si se utiliza la codificación de corrección de errores, se tendría que aplicar la interferencia forzada a más bits para garantizar la destrucción de un paquete. Esto destruiría uno o una pluralidad de bits en algún lugar del paquete haciendo que el paquete, por ejemplo, sea ignorado debido a que se destruyó la palabra de sincronización, se llene con un contenido completamente sin sentido o no supere la verificación de

redundancia cíclica (CRC). Sin embargo, estos efectos no se detectan automáticamente como una situación de interferencia forzada.

El diagrama de la Fig. 4 ilustra una situación que comienza con la recepción de una señal de radiocomunicaciones normal durante cuatro periodos de tiempo consecutivos, incluyendo cada periodo de tiempo T_n un segmento de información. En el formato de señal utilizado en la Fig. 4, un segmento de información se extiende durante un período de tiempo de T_b . El valor del nivel de potencia de cada período de tiempo se denomina P_m . Normalmente hay una variación de los valores de potencia P_m recibidos a lo largo del tiempo. Se determina continuamente un valor estadístico P_d de los niveles de potencia P_m medidos sobre la base de niveles de potencia de segmentos de información recibidos previamente. En varias realizaciones, P_m se mide durante un período de tiempo limitado T_m , como 1 s.

Uno de los valores estadísticos básicos es un valor de media, como se indica con una línea discontinua en la Fig. 4, que indica que el nivel de potencia recibido puede aumentar o disminuir con el tiempo. El valor de media se determina de forma continua sobre la base de niveles de potencia de segmentos de información recibidos previamente o se determina de forma continua para cada segmento de información. En varias realizaciones, el valor estadístico es la desviación estándar de un conjunto o de todos los valores de nivel de potencia P_m . El conjunto de valores de nivel de potencia puede basarse en una pluralidad de valores, valores medidos durante un período de tiempo, o la totalidad o un subconjunto de valores de un segmento de información específico.

En el momento t_j se emite y recibe una señal 44 de interferencia forzada durante un período de tiempo en el que también se emite un segmento de información. La señal 44 de interferencia forzada tiene un nivel de potencia P_j que es diferente del nivel de potencia P_m del segmento de información y también diferente del valor de media P_d . El nivel de potencia P_j es mayor que el nivel de potencia medio. La diferencia es P_e . Si el nivel de potencia P_j se desvía más del valor de media o del valor estadístico que un valor de referencia o umbral, se determina que el nivel de potencia P_j indica que se han producido medidas de perturbaciones radioeléctricas intencionadas o no intencionadas. Como resultado, se genera una señal de alarma. El valor umbral puede ser de dos a cinco veces la desviación estándar o preferiblemente alrededor de tres veces la desviación estándar.

Un detector 44 para detectar medidas de perturbaciones radioeléctricas intencionadas o no intencionadas está conectado a una ubicación apropiada en una cadena de recepción donde la medición se puede realizar con un ancho de banda lo suficientemente alto (la velocidad de medición de potencia debe ser del orden de la tasa de bits de la señal recibida, pero se podrá usar cualquier ancho de banda que permita más de una medición por segmento de información). La ubicación exacta depende de la arquitectura del receptor. El detector producirá una señal de alerta cuando se detecten medidas de perturbaciones radioeléctricas intencionadas o no intencionadas.

En un receptor analógico como se muestra en la Fig. 5, una antena 46 está conectada a un Amplificador de Bajo Ruido (LNA) 48 de manera convencional. Una salida del LNA 48 está conectada a un mezclador 50 que mezcla la señal amplificada con una señal de frecuencia ajustable de un oscilador 52. El mezclador está conectado también a una etapa de Frecuencia Intermedia con un amplificador (IF AMP) 54, una de cuyas salidas está conectada a un filtro 56 de manera convencional.

En la realización que se muestra en la Fig. 5, el IF AMP 54 comprende un Control Automático de Ganancia (AGC) 58. En varias realizaciones, el AGC 58 genera una señal que es indicativa de la potencia de la señal recibida. La señal generada se envía al detector 44 a través de una salida del AGC 58 que está conectada al detector 44. Una salida del filtro 56 está conectada a un convertidor analógico a digital (ADC) 60 que proporciona un flujo continuo de bits de datos digitales y una salida de nivel de potencia. La salida de nivel de potencia está conectada al detector 44. Una señal en la salida de nivel de potencia es indicativa de la potencia de la señal recibida y, por lo tanto, puede usarse para detectar medidas de perturbaciones radioeléctricas intencionadas o no intencionadas.

En un receptor digital, como se muestra en la Fig. 6, la antena 46 está conectada al LNA 48 de manera convencional. La señal amplificada en el LNA 48 se procesa en el ADC proporcionando un flujo continuo de bits de datos digitales y una salida de nivel de potencia. La salida de nivel de potencia está conectada al detector 44. Una señal en la salida de nivel de potencia es indicativa de la potencia de la señal recibida y, por lo tanto, puede usarse para detectar medidas de perturbaciones radioeléctricas intencionadas o no intencionadas.

En la Fig. 7 se muestran los componentes básicos de una realización de un detector 44 de acuerdo con la invención. El detector 44 podría ser un dispositivo físico o implementarse mediante *software*. Un detector 62 de nivel de potencia está conectado a una posición apropiada en un receptor de radiocomunicaciones para detectar continuamente una señal de nivel de potencia indicativa de la potencia de segmentos de información en una señal de radiocomunicaciones recibida. Un detector 63 de reloj de bits está conectado a una posición apropiada en un receptor de radiocomunicaciones para detectar continuamente un reloj de bits con el fin de proporcionar una base para la sincronización. Los valores de los niveles de potencia son procesados por una unidad 64 de procesamiento y almacenados en una unidad 66 de memoria. En diversas realizaciones, el procesamiento de los niveles de potencia comprende calcular al menos un valor estadístico. Normalmente, se calcula continuamente un valor de media de los valores del nivel de potencia.

En varias realizaciones, el detector 62 de nivel de potencia está conectado a una posición apropiada en un receptor de radiocomunicaciones para detectar continuamente una señal de nivel de potencia indicativa de la potencia de segmentos de información independientes en una señal de radiocomunicaciones recibida. El detector 44 también se puede usar para medir continuamente la potencia de un paquete de datos recibido y para detectar si debe producirse algún escalón en la potencia. Tan pronto como se detecta el inicio de un paquete, comienza una evaluación de la potencia. Independientemente de la sincronización de bits, se generará una alarma, en caso de que haya un escalón de potencia positivo o negativo.

El procesamiento comprende además comparar repetidamente un valor actual del nivel de potencia de al menos un segmento de información de una señal recibida con dicho valor estadístico. Cuando un valor de nivel de potencia actual, o un conjunto de valores de nivel de potencia recibidos recientemente, difiere del valor estadístico en más de un valor umbral, se considera que hay presencia de medidas de perturbaciones radioeléctricas intencionadas o no intencionadas. Cuando el procesamiento da como resultado la detección de medidas de perturbaciones radioeléctricas intencionadas o no intencionadas, la unidad 64 de procesamiento ordena a una unidad 68 de salida que produzca una señal de alerta y que reenvíe la señal de alerta a una unidad central, como se describe con más detalle a continuación.

En la Fig. 8 se muestra una instalación básica de un sistema de radiocomunicaciones. Esta realización se refiere a un sistema de alarma doméstico que comprende una primera pasarela 12, una segunda pasarela 12' y al menos un dispositivo periférico inalámbrico, como un detector 14 de infrarrojos. La primera pasarela 12, la segunda pasarela 12' y el detector 14 de infrarrojos se comunican todos mediante radiocomunicaciones. Al menos una pasarela se comunica repetidamente con la estación 22 de monitorización central remota como se ha dado a conocer anteriormente. Un dispositivo bloqueador 70 de *sniping* se ha movido a una posición en la que se pueden recibir señales de radiocomunicaciones en la instalación y se pueden tomar medidas de perturbaciones radioeléctricas.

Las pasarelas primera y segunda 12, 12' comprenden primeras unidades 72 de comunicación y segundas unidades 74 de comunicación. Las primeras unidades 72 de comunicación se utilizan para comunicarse con la estación 22 de monitorización central remota bien a través de una conexión 24 por cable o bien a través de una conexión inalámbrica tal como el GSM o una red celular digital similar. La conexión con la estación 22 de monitorización central remota también puede ser a través de una conexión por cable, como una red telefónica pública conmutada o internet.

Las segundas unidades 74 de comunicación se utilizan principalmente para la comunicación dentro de la instalación entre pasarelas y entre pasarelas y nodos periféricos. Cada pasarela está controlada por una unidad central 76 y comprende una unidad 78 de alimentación, normalmente una batería. Al menos una pasarela está provista de un detector 44 que monitoriza continuamente la radiocomunicación recibida en la pasarela. Cuando el detector 44 detecta medidas de perturbaciones radioeléctricas intencionadas o no intencionadas en el sistema de radiocomunicaciones, se transfiere una señal de alerta a la unidad central 76. Entonces se puede generar una señal de alarma en la pasarela y la misma se puede reenviar a la estación 22 de monitorización central remota de manera apropiada.

Al combinar los datos de potencia con el flujo de bits continuo, es posible detectar medidas de perturbaciones radioeléctricas intencionadas o no intencionadas. La tabla de la Fig. 9 describe una parte de un paquete recibido correctamente con los bits como "1" y "0" en la fila superior y el nivel de energía como "A" a "Z" en la segunda fila. En la tabla de la Fig. 10 está presente una activación de *sniping* de paquetes. Los niveles de energía más altos durante la interferencia forzada de paquetes se indican con una **V** dando como resultado un flujo continuo de bits diferente y alterado.

Un escalón de potencia se detectaría fácilmente y emparejando el escalón de potencia con el patrón de bits antes y después del escalón de potencia se puede determinar que había un paquete en camino al receptor que se sometió a *sniping*. La detección del *sniping* también podría basarse únicamente en cambios breves de la potencia si el flujo continuo de bits recibido ignora el factor de reconocimiento de paquetes, aunque lo más probable es que esto provocaría algunas falsas alarmas, ya que los sistemas vecinos y otros protocolos de RF podrían confundirse con *snipers*.

Si el método se ejecuta en dos rutas de recepción independientes (por ejemplo, en sistemas con diversidad de Rx o conmutación de antena receptora), también sería posible detectar *snipers* que intenten imitar el nivel de potencia de las señales recibidas para enmascarar el *sniper*. Este tipo de bloqueador tendría que ser muy sofisticado y conocer la ubicación del receptor, el transmisor y su relación con ambos. También tendría que tener un conocimiento detallado del RSSI del receptor en relación con el transmisor. La señal del *sniper* no se recibiría con la misma intensidad en ambos receptores e incluso si el *sniper* tuviera una potencia perfectamente adaptada a uno de los receptores, estaría fuera de fase y de potencia con el otro.

En varias realizaciones, el cálculo del valor estadístico comprende el cálculo de una desviación estándar de los valores del nivel de potencia de segmentos de información independientes. Mediante el uso de la desviación estándar, pueden seguir gestionándose situaciones en las que los niveles de potencia varían normalmente sin producir una cantidad demasiado alta de señales de alerta y alarma fallidas. Si un valor de nivel de potencia actual se desvía más de tres veces la desviación estándar, es muy probable que se hayan cogido medidas de perturbaciones radioeléctricas intencionadas o no intencionadas. Es posible utilizar también un umbral del doble de la desviación estándar o igual a la desviación estándar para producir la señal de alerta y alarma.

REIVINDICACIONES

1. Un método de detección de perturbaciones radioeléctricas en un sistema de radiocomunicaciones de un sistema de alarma y seguridad de un edificio, comprendiendo el sistema de radiocomunicaciones un dispositivo (12) de pasarela y un dispositivo periférico (14, 16), cada uno dispuesto para enviar señales de radiocomunicaciones hacia el otro y para recibir señales de radiocomunicaciones del otro, estando las señales de radiocomunicaciones en forma de segmentos de información independientes transmitidos como paquetes de datos en el dominio del tiempo, comprendiendo el método los pasos:
 - i. medir en el dispositivo (12) de pasarela el nivel de potencia (P_m) de segmentos de información independientes de las señales de radiocomunicaciones recibidas desde el dispositivo periférico (14, 16), para obtener valores de nivel de potencia medidos;
 - ii. determinar un valor estadístico (P_d) de los valores de nivel de potencia medidos para los segmentos de información independientes;
 - iii. comparar un nivel de potencia medido seleccionado con el valor estadístico; y
 - iv. producir una señal de alerta, que indica una perturbación radioeléctrica, si la diferencia entre el nivel de potencia medido seleccionado y el valor estadístico supera un umbral.
2. El método según la reivindicación 1, en el que el dispositivo (12) de pasarela y el dispositivo periférico (14, 16) se comunican con información dividida en una pluralidad de segmentos de información y cada uno de dichos segmentos de información se comunica durante un tiempo (T_b) donde dicho valor estadístico (P_d) y dichos valores de nivel de potencia (P_m) se actualizan repetidamente.
3. El método según cualquiera de las reivindicaciones anteriores, en el que dicho valor estadístico (P_d) es la desviación estándar y el valor umbral es más menos tres veces dicha desviación estándar.
4. El método según cualquiera de las reivindicaciones anteriores, en el que dicho sistema de radiocomunicaciones es un sistema de alarma doméstico.
5. El método según la reivindicación 1, en el que dicho valor estadístico (P_d) es el valor de media de valores del nivel de potencia (P_m) durante un período de tiempo predeterminado (T_m) y el valor umbral es más menos dos a cinco veces dicho valor de media.
6. El método según una cualquiera de las reivindicaciones anteriores, en el que la señal de nivel de potencia se obtiene en un ancho de banda correspondiente a un orden de segmentos de información independientes en una señal de radiocomunicaciones recibida en dicho receptor.
7. El método según una cualquiera de las reivindicaciones anteriores, que comprende además medir la potencia de una señal de radiocomunicaciones entrante a un receptor de radiocomunicaciones en una unidad de Control Automatizado de Ganancia (AGC) del receptor.
8. El método según una cualquiera de las reivindicaciones 1 a 6, que comprende además medir la potencia de una señal de radiocomunicaciones entrante a un receptor de radiocomunicaciones en un convertidor analógico a digital (ADC).
9. El método según una cualquiera de las reivindicaciones anteriores, que comprende además medir la recepción de la señal del nivel de potencia en dicho receptor de señales de radiocomunicaciones de la pasarela.
10. Un detector (44) para detectar perturbaciones radioeléctricas en un sistema de radiocomunicaciones de un sistema de alarma y seguridad de un edificio, comprendiendo el sistema de radiocomunicaciones un dispositivo (12) de pasarela y un dispositivo periférico (14, 16), cada uno dispuesto para enviar señales de radiocomunicaciones al otro y para recibir señales de radiocomunicaciones del otro, estando las señales de radiocomunicaciones en forma de segmentos de información independientes transmitidos como paquetes de datos en el dominio del tiempo, en donde el detector (44) comprende:
 - un detector (62) de nivel de potencia,
 - una unidad (64) de procesamiento conectada operativamente al detector (62) de nivel de potencia,
 - una unidad (66) de memoria que almacena una pluralidad de valores estadísticos de niveles de potencia detectados, en el que dicha unidad (64) de procesamiento está dispuesta para:
 - i. medir en el dispositivo (12) de pasarela el nivel de potencia (P_m) de segmentos de información independientes de las señales de radiocomunicaciones recibidas desde el dispositivo periférico (14, 16),

- ii. determinar un valor estadístico (Pd) de valores de nivel de potencia medidos para los segmentos de información independientes,
 - iii. comparar un nivel de potencia medido seleccionado con el valor estadístico,
 - iv. producir una señal de alerta, que indica una perturbación radioeléctrica, si la diferencia entre el nivel de potencia medido seleccionado y el valor estadístico supera un umbral.
- 5
11. El detector según la reivindicación 10, en el que el detector (62) de nivel de potencia está conectado a un convertidor analógico a digital, ADC, del receptor de señales de radiocomunicaciones.
12. El detector según la reivindicación 10, en el que el detector (62) de nivel de potencia está conectado a una unidad de Control Automatizado de Ganancia, AGC, del receptor.
- 10
13. El detector según una cualquiera de las reivindicaciones 10 a 12, en el que el detector (44) está conectado operativamente al receptor de señales de radiocomunicaciones de la pasarela.
14. El detector según una cualquiera de las reivindicaciones 10 a 13, en el que el detector (44) está provisto de una primera entrada que recibe el nivel de potencia de la potencia de segmentos de información independientes en una señal de radiocomunicaciones recibida en dicho receptor de señales de radiocomunicaciones, y de una segunda entrada que recibe segmentos de información independientes en una señal de radiocomunicaciones recibida en dicho receptor.
- 15

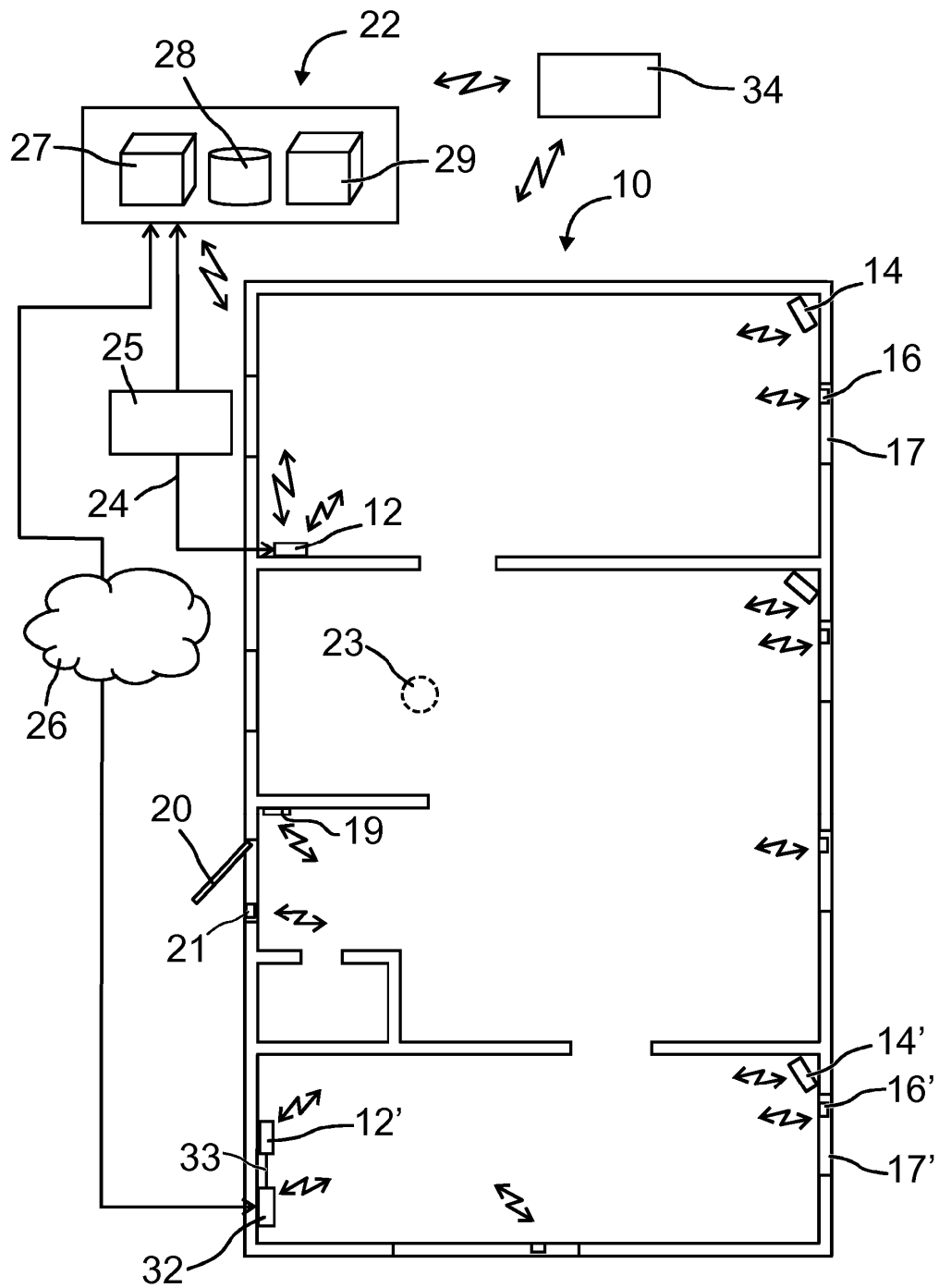


Fig. 1

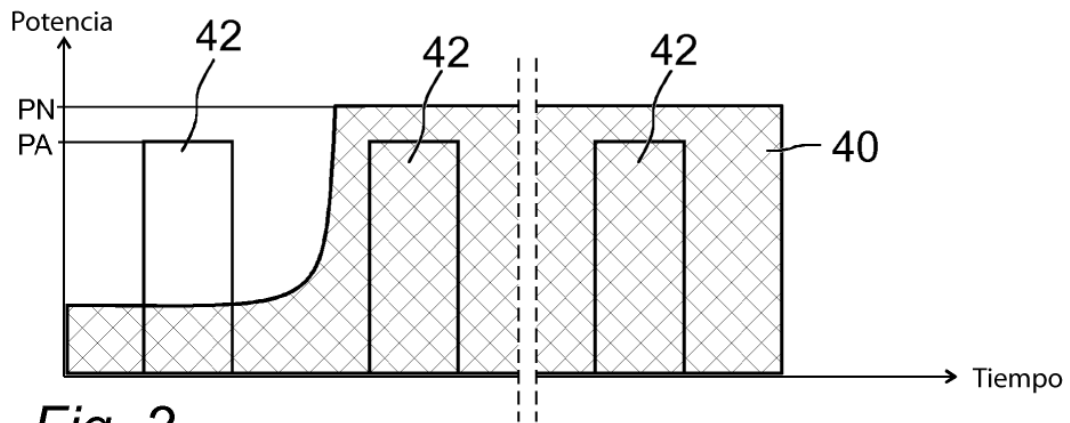


Fig. 2

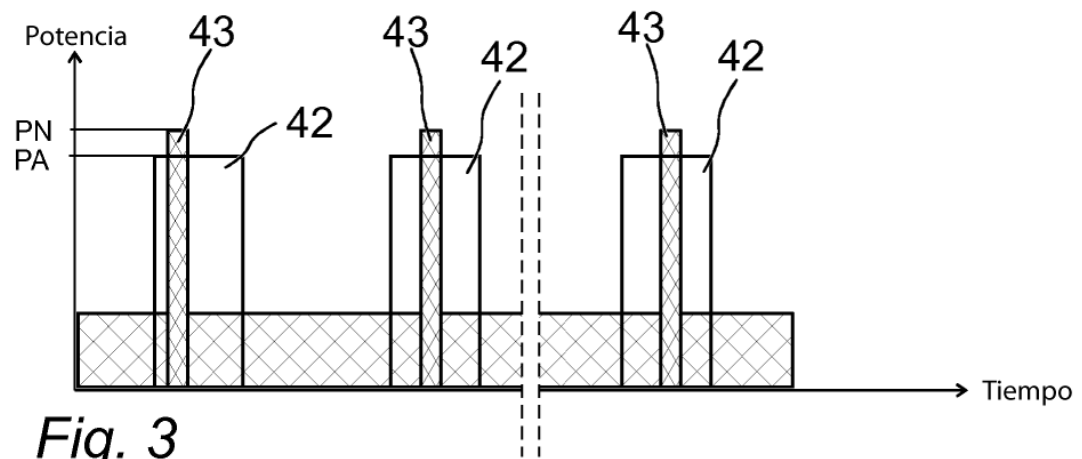


Fig. 3

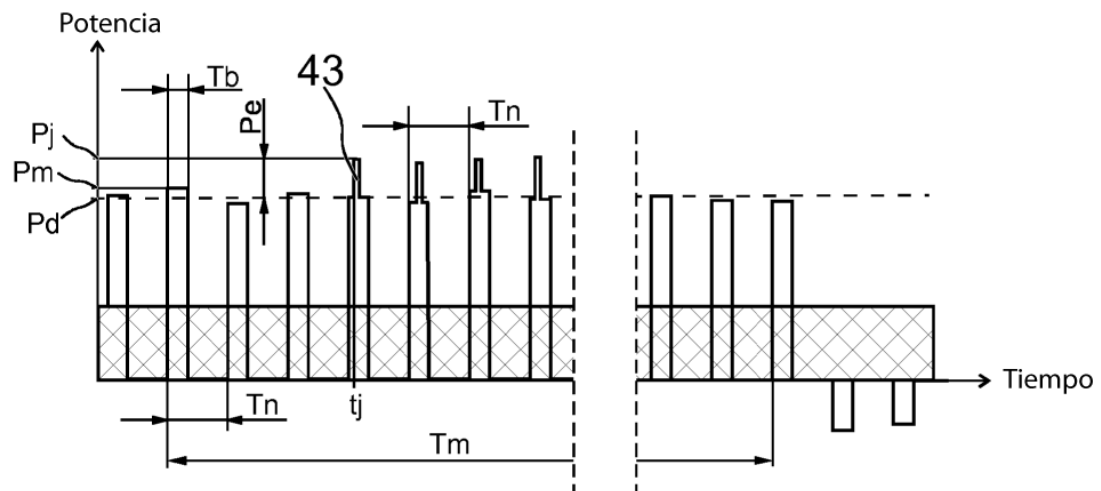
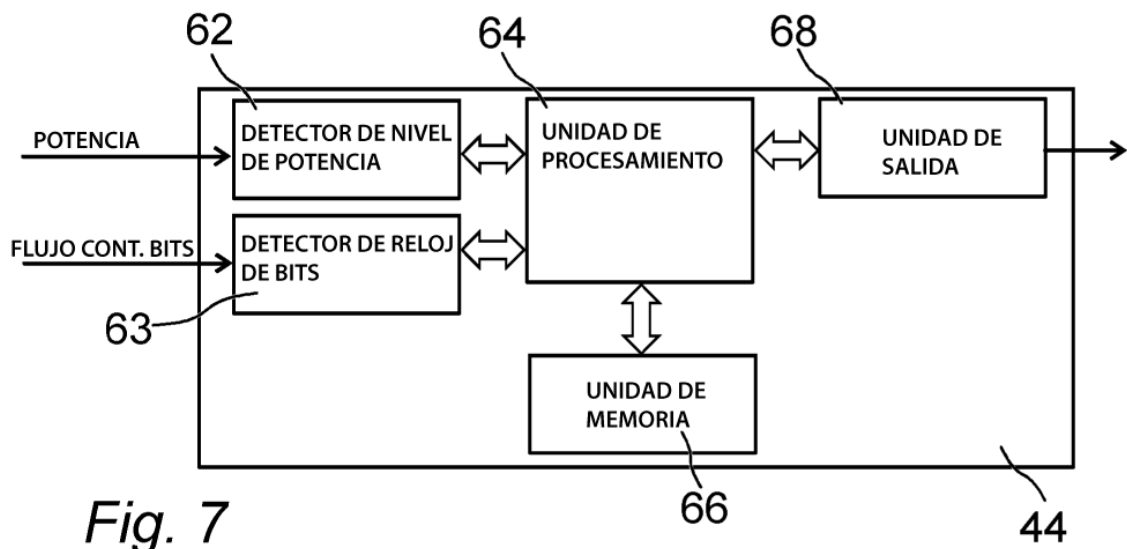
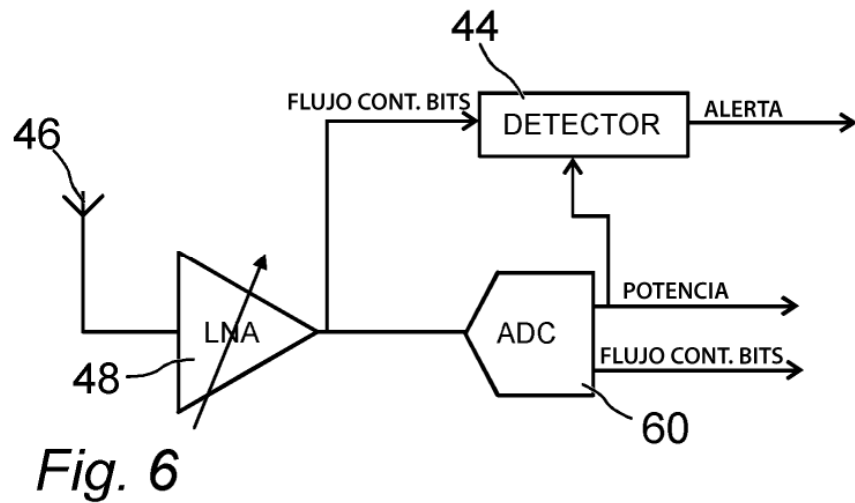
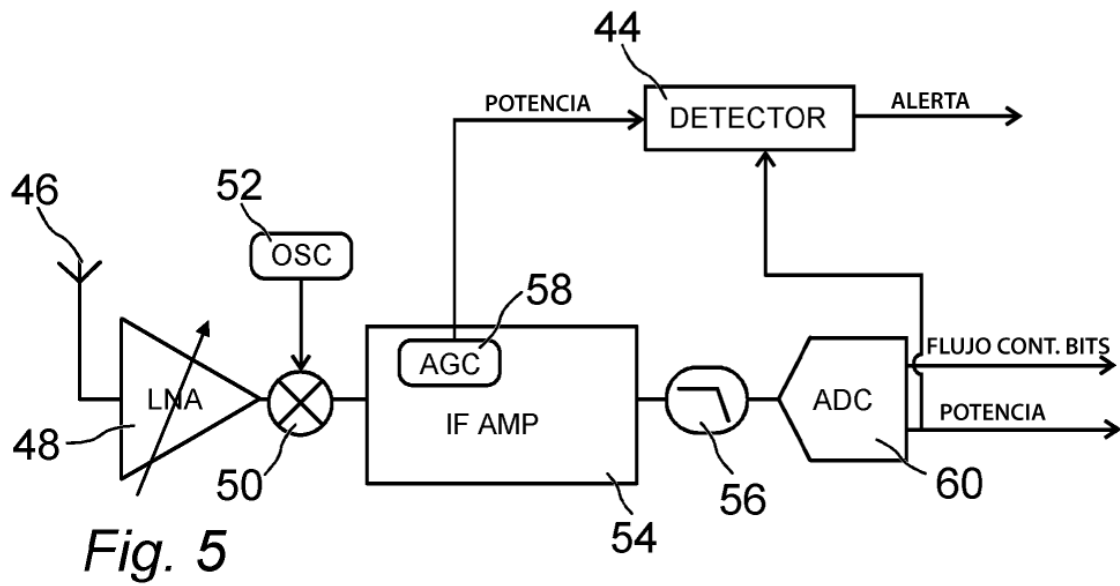
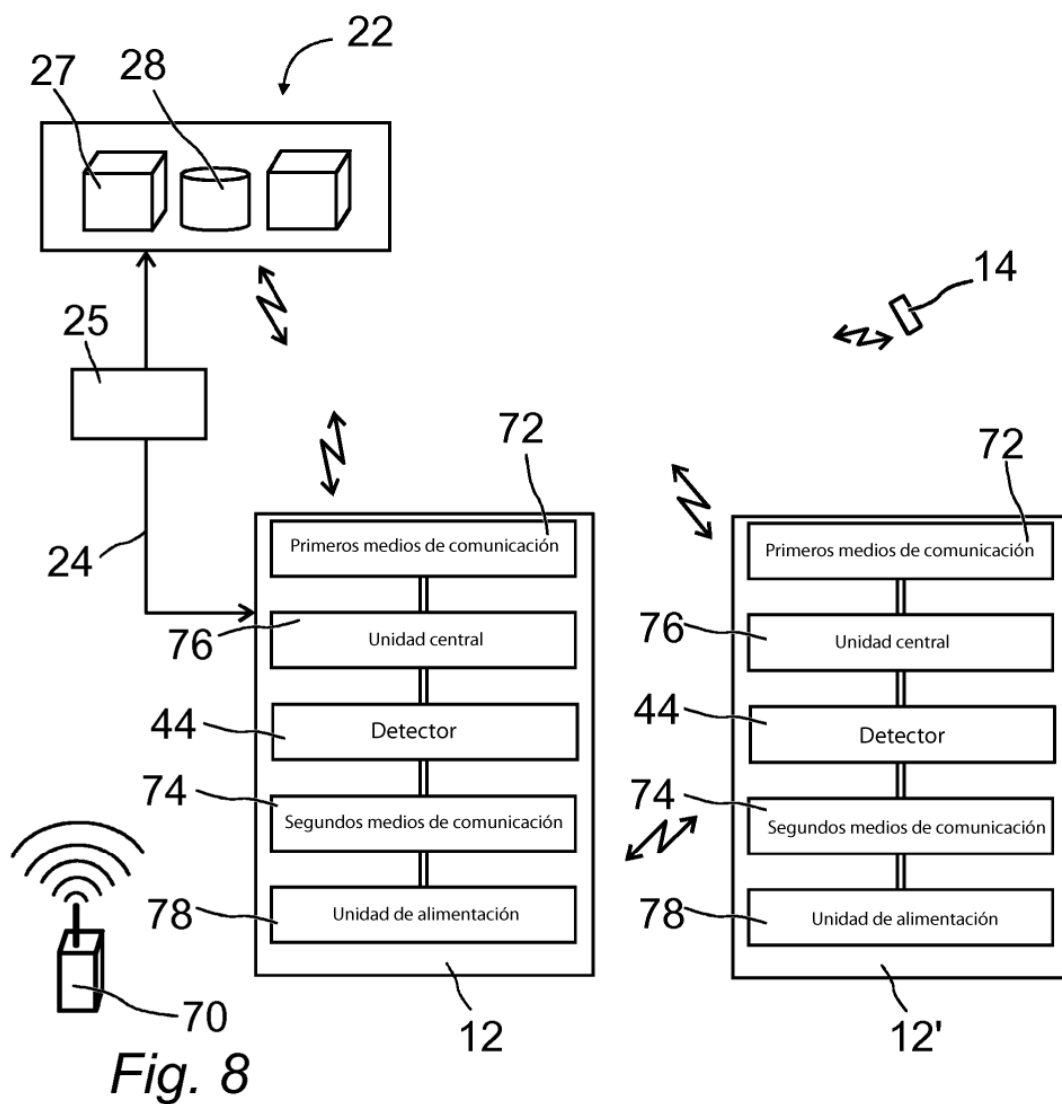


Fig. 4





1	0	1	0	1	0	1	1	0	0	1	0	1	1	0	1
G	G	G	G	H	H	H	H	H	G	G	G	G	G	G	G

Fig. 9

1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1
G	G	G	G	H	H	H	V	V	V	V	V	V	V	G	G

Fig. 10