(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 332 428**

(51) Int. Cl.:
H04L 1/18 (2006.01)
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07008550 .1**
(96) Fecha de presentación : **26.04.2007**
(97) Número de publicación de la solicitud: **1850523**
(97) Fecha de publicación de la solicitud: **31.10.2007**

(54) Título: **Procedimiento y aparato para la sincronización de parámetros de descifrado en un dispositivo de comunicaciones inalámbrico.**

(30) Prioridad: **27.04.2006 US 745750 P**

(45) Fecha de publicación de la mención BOPI:
04.02.2010

(45) Fecha de la publicación del folleto de la patente:
04.02.2010

(73) Titular/es: **Innovative Sonic Limited**
Offshore Incorporations Centre
Road Town, P.O. Box 957
Tortola, VG

(72) Inventor/es: **Jiang, Sam, Shiaw-Shiang**

(74) Agente: **Zea Checa, Bernabé**

DESCRIPCIÓN

Procedimiento y aparato para la sincronización de parámetros de descifrado en un dispositivo de comunicaciones inalámbrico.

La presente invención se refiere a un procedimiento y a un aparato para la sincronización de parámetros de descifrado en un dispositivo de comunicaciones inalámbrico según los preámbulos de las reivindicaciones 1 y 4.

En un sistema de comunicaciones inalámbrico, para proteger los datos de usuario y las señales de información de que sean interceptados por dispositivos no autorizados, la técnica anterior puede realizar una encriptación en paquetes transmitidos entre un emisor y un receptor a través un procedimiento de cifrado/descifrado. En primer lugar, el emisor genera datos de una secuencia de claves a través de un algoritmo especificado en base en claves de cifrado (CK), el cifrado de números de secuencia (SN), y otros parámetros o variables, y encripta datos en texto plano con la secuencia de claves para generar datos de texto cifrado. El receptor puede descifrar los datos de texto cifrado a través de inversas operaciones, de modo que el CK es importante. Además del CK, el cifrado de SN es otro parámetro importante utilizado para el cifrado de datos en el sistema de comunicaciones inalámbrico. El cifrado de SN está formado por números de secuencia. Por ejemplo, en un sistema de telecomunicaciones de tercera generación (3G), el cifrado de SN, denominado SN global, está compuesto por un número de hipertrama de control de conexión de radio de 20 bits (RLC HFN) y un número de secuencia de control de conexión de radio de 12 bits (RLC SN).

Se supone que el SN global va con el paquete a través de una red inalámbrica sin cifrar, para así mantener la sincronización y la precisión de la transmisión de señales entre el emisor y el receptor. El SN global es un encabezado para el cifrado. Para reducir el encabezado, la técnica anterior divide el SN global en dos partes, una que se denomina SN integrado en la cabecera de un paquete, y el otro es un HFN almacenado tanto en el emisor como en el receptor. El HFN es similar a llevar número de SN. Cada vez que el SN reinicia su valor de representación máximo de nuevo a 0, el HFN es incrementado en una unidad en el emisor y en el receptor. Por ejemplo, si el SN está representado por 7 bits, que va de 0 a 127, una vez que el SN se encuentra más allá de 127, el HFN se incrementa en 1, y el SN vuelve a comenzar desde 0. En consecuencia, según el SN, el emisor y el receptor pueden incrementar oportunamente = HFN, para así mantener la sincronización del HFN y mantener procesos de cifrado y descifrado.

Para asegurar el correcto mantenimiento de los HFNs, puede utilizarse una ventana deslizante si la capa inferior soporta el suministro fuera de secuencia. Existen dos tipos de ventana deslizante, de tipo "*Push*" y de tipo "*Pull*". La ventana de tipo "*Push*" es como una ventana de recepción utilizada en la entidad RLC AM en UMTS (sistema universal de telecomunicaciones móviles) según se especifica en 3GPP TS 25.322 "*Radio Link Control protocol specification*". La ventana tipo "*Push*" avanza solamente cuando se recibe con éxito o se informa que se descarte un paquete que corresponde al borde inferior de la ventana. Cuando hay un paquete con SN fuera de la ventana de tipo "*Push*", el paquete se descarta. La ventana de tipo "*Pull*" es como la ventana de recepción utilizada en la entidad de reordenamiento de HSDPA (acceso a descarga de paquetes a alta velocidad) en UMTS según se especifica en 3GPP TS 25.321 "*Medium Access Control protocol specification*". La ventana de tipo "*Pull*" avanza cuando se recibe un paquete con SN y el SN se establece para que sea el borde superior actualizado de la ventana de tipo "*Pull*".

En la técnica anterior, el tipo de ventana y el tamaño de ventana de la ventana deslizante para el objetivo de identificar un valor de HFN para el descifrado no se especifica cuidadosamente. Si no se utilizan correctamente, los HFN pueden quedar fuera de sincronización entre el emisor y el receptor.

Por ejemplo, si suponemos que los tamaños de ventana de las ventanas de recepción utilizadas para la entidad HARQ (petición de repetición automática híbrida) y la entidad RLC son 10 y 16 en un receptor UMTS, y la ventana de tipo "*Pull*" se utiliza para una entidad de descifrado de la entidad PDCP (protocolo de convergencia de datos en paquetes) con un tamaño de ventana = 10. Si se reciben con éxito paquetes con SN = 0 ~ 9 excepto el paquete con SN = 0, entonces la ventana de recepción de la entidad de descifrado abarca de 0 a 9. Ahora, si se recibe un paquete con SN =10, la ventana de recepción de la entidad de descifrado avanza para extenderse de 1 a 10. Supóngase que el SN = 0 omitido se debe a un error residual de HARQ, tal como un error "*NACK_to_ACK*" (no reconocimiento a reconocimiento) o un error "*DTX_to_ACK*" (transmisión discontinua a reconocimiento), de modo que la entidad RLC active la retransmisión del paquete con SN = 0. Supóngase que se retransmite el paquete con SN = 0 después de un estado de "*NACK*" reportado por la entidad RLC y se recibe con éxito. El paquete con SN = 0 se envía después a la entidad de descifrado. Como que el SN = 0 ahora se encuentra ahora fuera de la ventana de recepción de la entidad de descifrado, la entidad de descifrado toma SN 0 para que pertenezca al siguiente ciclo SN, y la ventana de tipo "*Pull*" avanzará la ventana con HFN incrementado. Tras ello, el HFN quedará fuera de sincronización entre el receptor y el emisor.

Por otra parte, supóngase que la ventana de tipo "*Push*" se utiliza para la ventana de recepción de la entidad de descifrado con tamaños de ventana = 10 en el ejemplo anterior. Si se reciben con éxito paquetes con SN = 0 ~ 9 excepto el paquete con SN = 0, entonces la ventana de recepción de la entidad de descifrado abarca de 0 a 9. Ahora, si se recibe un paquete con SN =10, la ventana de tipo "*Push*" no tendrá en cuenta y descartará este paquete ya que se encuentra fuera de la ventana. Después de ello, como que la entidad RLC no realizará una petición para la retransmisión de SN = 10, la ventana en la entidad de descifrado se detendrá.

Por lo tanto, la presente invención tiene como objetivo disponer un procedimiento y un aparato para la sincronización de parámetros de descifrado en un dispositivo de comunicaciones inalámbrico que reduzca las señales de encabezado y evite desperdiciar recursos de radio.

Esto se consigue mediante un procedimiento y un aparato para la sincronización de parámetros de descifrado en un dispositivo de comunicaciones inalámbrico según las reivindicaciones 1 y 4. Las reivindicaciones dependientes pertenecen a otros desarrollos y mejoras correspondientes.

Tal como se verá más claramente a partir de la descripción detallada que se da a continuación, el procedimiento reivindicado para la sincronización de parámetros de descifrado en un extremo de recepción de un sistema de comunicaciones inalámbrico comprende establecer una primera entidad y una segunda entidad dentro del extremo de recepción, y disponer una ventana de recepción de la primera entidad como ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual que el tamaño de ventana de una ventana de recepción de una segunda entidad, en el que la primera entidad realiza una función de descifrado, y la segunda entidad es una entidad de control de conexión de radio.

A continuación, la invención se ilustra también a modo de ejemplo, haciendo referencia a los dibujos que se acompañan, en los cuales:

La figura 1 es un diagrama de bloques funcional de un dispositivo de comunicaciones.

La figura 2 es un diagrama del código del programa mostrado en la figura 1.

La figura 3 es un diagrama de flujo de un proceso de acuerdo con la realización preferida de la presente invención.

Hágase referencia a la figura 1, que es un diagrama de bloques funcional de un dispositivo de comunicaciones 100. Por motivos de brevedad, la figura 1 solamente muestra un dispositivo de entrada 102, un dispositivo de salida 104, un circuito de control 106, una unidad central de proceso (CPU) 108, una memoria 110, un código de programa 112, y un transceptor 114 del dispositivo de comunicaciones 100. En el dispositivo de comunicaciones 100, el circuito de control 106 ejecuta el código del programa 112 en la memoria 110 a través de la CPU 108, controlando así una operación del dispositivo de comunicaciones 100. El dispositivo de comunicaciones 100 puede recibir la entrada de señales de un usuario a través del dispositivo de entrada 102, tal como un teclado, y puede enviar imágenes y sonidos a través del dispositivo de salida 104, tal como un monitor o altavoces. El transceptor 114 se utiliza para recibir y transmitir señales inalámbricas, suministrando señales recibidas al circuito de control 106, y señales de salida generadas por el circuito de control 106 de manera inalámbrica. Desde una perspectiva de un marco de protocolos de comunicaciones, el transceptor 114 puede verse como una parte de la Capa 1, y el circuito de control 106 puede utilizarse para realizar funciones de Capa 2 y Capa 3. Preferiblemente, el dispositivo de comunicaciones 100 se utiliza en un sistema de comunicaciones móviles de tercera generación (3G).

Continúese haciendo referencia a la figura 2. La figura 2 es un diagrama del código del programa 112 mostrado en figura 1. El código del programa 112 incluye una capa de aplicación 200, una Capa 3 202, y una Capa 2 206, y se conecta a una Capa 1 218. La Capa 2 206 comprende dos subcapas: una primera entidad de subcapa 224 y una segunda entidad de subcapa 226. La primera entidad de subcapa 224 realiza operaciones de cifrado y descifrado de acuerdo con parámetros o variables de clave de cifrado, SN de cifrado, etc. La segunda entidad de subcapa 226 puede ser una combinación de una entidad RLC y una entidad MAC (control de acceso al medio).

Hágase referencia a la figura 3, que es un diagrama de flujo de un proceso 50 de acuerdo con la realización preferida de la presente invención. El proceso 50 se utiliza en el dispositivo de comunicaciones para sincronizar un parámetro de cifrado, y puede compilarse en el código del programa de configuración de la ventana de recepción 220. El proceso 50 comprende las siguientes etapas:

Etapa 500: Inicio.

Etapa 502: Establecer la ventana de recepción de la primera entidad de subcapa 224 como ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual al tamaño de ventana de la ventana de recepción de la segunda entidad de subcapa 226.

Etapa 504: Fin.

De acuerdo con el proceso 50, la ventana de recepción de la primera entidad de la subcapa 224 se establece que sea una ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual que el tamaño de ventana de la ventana de recepción de la segunda entidad de subcapa 226. Es decir, si se recibe un paquete con un SN fuera de la ventana de recepción de tipo "*Pull*", la ventana de recepción avanza, y el borde superior de la ventana de recepción se establece al SN. En esta situación, como que el tamaño de ventana de la ventana de recepción de la primera entidad de subcapa 224 es mayor o igual que el tamaño de ventana de la segunda entidad de subcapa 226, la extensión de la ventana de recepción de la primera entidad de subcapa 224 siempre cubre el SN que falta en la ventana de recepción de la segunda

entidad de subcapa 226. Por lo tanto, los SNs que se suministran fuera de secuencia por la segunda entidad de subcapa 226 se encontrarán siempre dentro de la ventana de recepción de la primera entidad de subcapa 224 para así mantener la sincronización de los valores del HFN para paquetes recibidos entre el emisor y el receptor.

Por ejemplo, supóngase que el tamaño de ventana de la ventana de recepción de la segunda entidad de subcapa 226 es 16 y la segunda entidad de subcapa 226 funciona en AM y soporta suministro fuera de secuencia. Por lo tanto, de acuerdo con el proceso 30, el tipo de ventana de la ventana de recepción de la primera entidad de subcapa 224 es de tipo "*Pull*" con un tamaño de ventana por lo menos igual a 16. Supóngase que se reciben con éxito paquetes con SN = 0 ~ 9 excepto el paquete con SN = 0. Los paquetes con SN = 1~9 serán suministrados a la primera entidad de subcapa 224 debido al suministro fuera de secuencia. La ventana de recepción de la primera entidad de subcapa 224 se extiende de 4090 a 9. Ahora, si la segunda entidad de subcapa 226 recibe un paquete con SN = 10 y el paquete se suministra a la primera entidad de subcapa 224 antes de que se reciba el SN = 0, el paquete será descifrado por la primera entidad de subcapa 224 y la ventana de recepción de la primera entidad de subcapa 224 avanza a intervalos de 4901 a 10. Es decir, SN = 0 se encuentra dentro de la ventana de recepción en comparación con el caso en el que SN = 0 se encontrará fuera de la ventana de recepción si el tamaño de ventana se establece que sea 10. Por lo tanto, cuando se recibe el paquete con SN = 0, la primera entidad de subcapa 224 puede descifrarlo con un HFN correcto de acuerdo con el proceso 50. El proceso 50 evita el problema de HFN fuera de sincronización.

Por lo tanto, utilizando el proceso 30, la ventana de recepción de la primera entidad de subcapa 224 es una ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual que el de la segunda entidad de subcapa 226, para así mantener la sincronización de los valores HFN.

REIVINDICACIONES

1. Procedimiento para la sincronización de parámetros de descifrado en un extremo de recepción de un sistema de comunicaciones inalámbrico, que comprende:

establecer una primera entidad y una segunda entidad dentro del extremo de recepción;

caracterizado por el hecho de que se establece una ventana de recepción de la primera entidad como ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual que un tamaño de ventana de una ventana de la recepción de la segunda entidad (502) en el que la primera entidad realiza una función de descifrado, y la segunda entidad es una entidad inferior de la primera entidad.

2. Procedimiento según la reivindicación 1, **caracterizado** por el hecho de que la segunda entidad es una entidad del control de conexión de radio.

3. Procedimiento según la reivindicación 1, **caracterizado** por el hecho de que la segunda entidad es una entidad del control de acceso al medio.

4. Dispositivo de comunicaciones (100) de un sistema de comunicaciones inalámbrico utilizado para manejar de manera eficaz el inicio de transmisión de enlaces de subida para evitar desperdiciar recursos de radio, que comprende:

un circuito de control (106) para realizar funciones del dispositivo de comunicaciones (100);

un procesador (108) instalado en el circuito de control (106) para ejecutar un código de programa (112) para operar el circuito de control (106); y

una memoria (110) conectada al procesador (108), para almacenar el código del programa (112);

en el que el procesador, al ejecutar el código del programa (112) está adaptado para establecer una primera entidad y una segunda entidad dentro del dispositivo de comunicaciones (100); **caracterizado** por el hecho de que el procesador, al ejecutar el código del programa (112) está adaptado para establecer una ventana de recepción de la primera entidad como ventana de tipo "*Pull*" con un tamaño de ventana mayor o igual que un tamaño de ventana de una ventana de recepción de la segunda entidad (502), en el que la primera entidad realiza una función de descifrado, y la segunda entidad es una entidad inferior de la primera entidad.

5. Dispositivo de comunicaciones según la reivindicación 4, **caracterizado** por el hecho de que la segunda entidad es una entidad de control de conexión de radio.

6. Dispositivo de comunicaciones según la reivindicación 4, **caracterizado** por el hecho de que la segunda entidad es una entidad de control de acceso al medio.

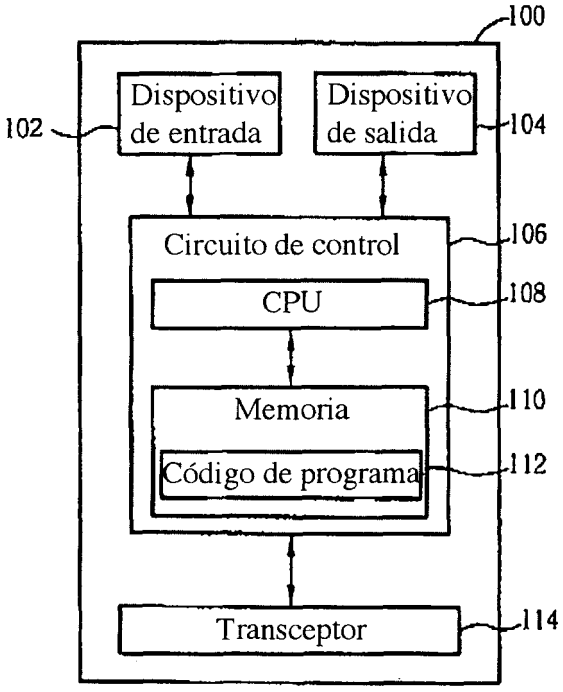
100
Dispositivo de entrada
102
Dispositivo de salida
104
Circuito de control
106
CPU
108
Memoria
110
Código de programa
112
Transceptor
114

Fig. 1

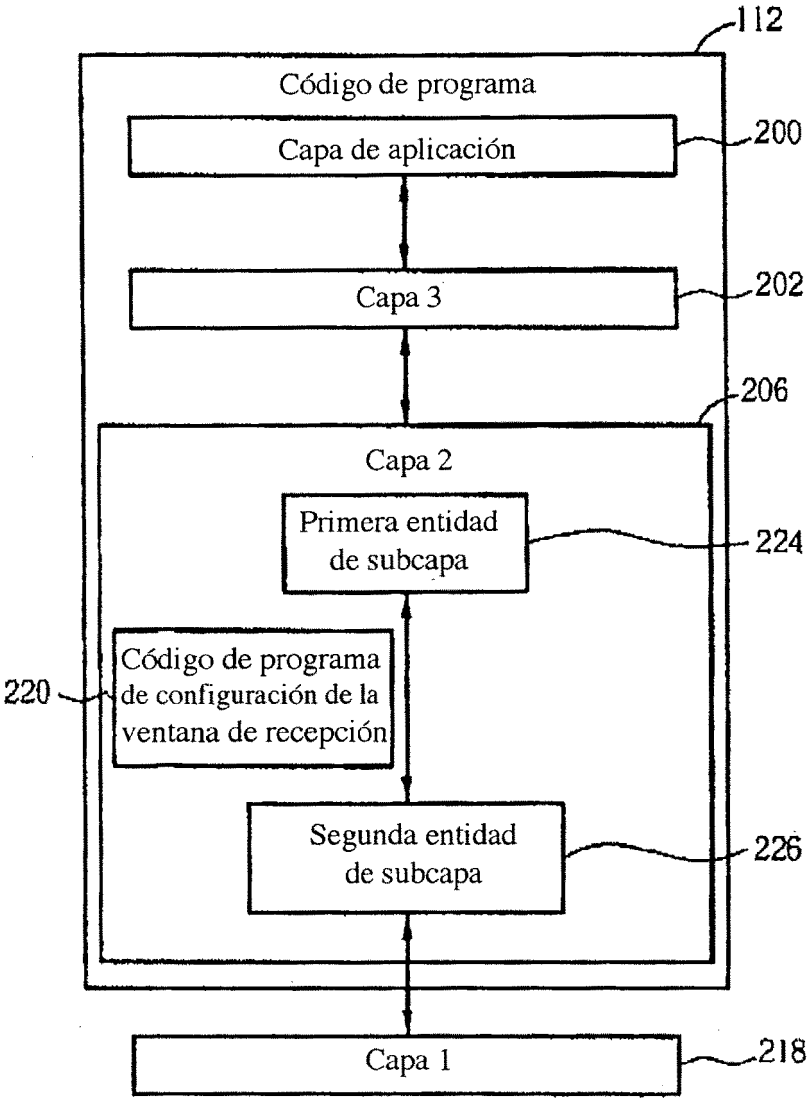
112
Código de programa
Capa de aplicación
200
Capa 3
202
206
Capa 2
Primera entidad de subcapa
224
Código de programa de configuración de la ventana de recepción
220
Segunda entidad de subcapa
226
Capa 1
218

Fig. 2

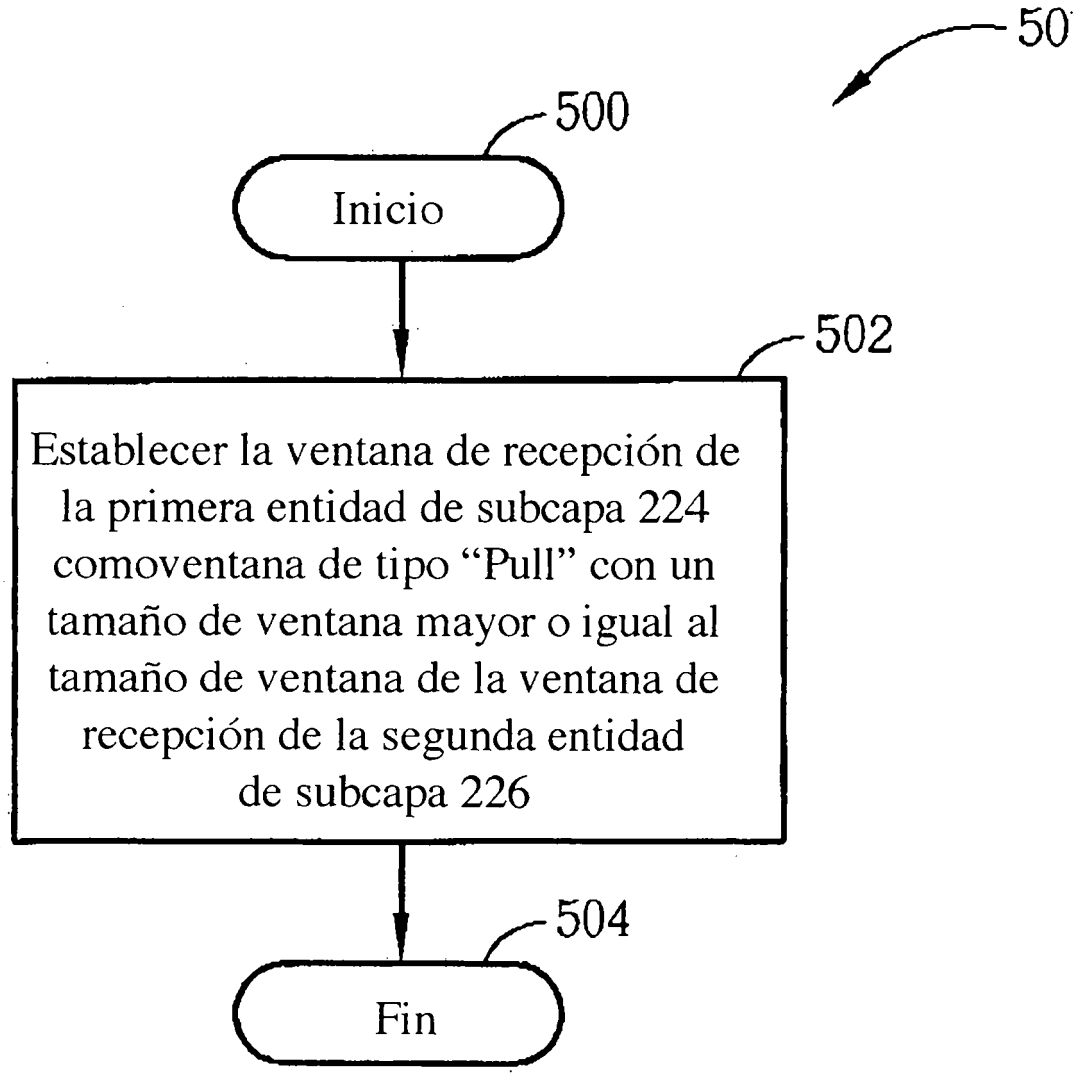
50
500
Inicio
502
Establecer la ventana de recepción de la primera entidad de subcapa 224 comoventana de tipo "Pull" con un tamaño de ventana mayor o igual al tamaño de ventana de la ventana de recepción de la segunda entidad de subcapa 226
504
Fin

Fig. 3