(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 576 108**

(51) Int. CI.:

H04W 52/02 (2009.01)
H04W 24/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.12.2009 E 09775145 (7)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2016 EP 2380382**

(54) Título: **Activación de un nodo de red desde un modo de servicio de reposo mediante verificación de un token de activación secreto recibido**

(30) Prioridad:

20.01.2009 DE 102009005187

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.07.2016

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
HOF, HANS-JOACHIM

(74) Agente/Representante:

LOZANO GANDIA, José

ACTIVACIÓN DE UN NODO DE RED DESDE UN MODO DE SERVICIO DE REPOSO MEDIANTE VERIFICACIÓN DE UN TOKEN DE ACTIVACIÓN SECRETO RECIBIDO

DESCRIPCIÓN

La invención se refiere a un procedimiento para activar un nodo de red a activar de una red inalámbrica.

Las redes inalámbricas, cuyos nodos comunican a través de una interfaz inalámbrica, se utilizan en diversos campos de aplicación. Por ejemplo sirven las redes inalámbricas de sensores o redes sensor-actuador para vigilar y controlar instalaciones de fabricación, de procesos químicos o para vigilar redes de tuberías. Los nodos sensores o bien nodos sensor-actuador comunican inalámbricamente entre sí mediante una interfaz de radio, para intercambiar valores de medida y órdenes de mando.

Tales redes inalámbricas incluyen la mayoría de las veces nodos de red cuya alimentación con energía la proporciona una batería contenida en el nodo. La vida útil o tiempo de funcionamiento de tales nodos de red operados por batería vienen limitados por la energía almacenada en la batería. Tan pronto como la batería está vacía, no pueden alimentarse con corriente eléctrica los circuitos contenidos en el nodo de red y dejan de funcionar. Para aumentar la vida útil de un nodo de red se traslada por lo tanto el nodo de red bajo determinadas circunstancias a un modo de funcionamiento de reposo, en el que se desactivan al menos en parte componentes y/o circuitos dentro del nodo de red, para reducir el consumo de energía del nodo de red. Allí está formada una de las configuraciones de circuitos del nodo de red para una red inalámbrica mediante la interfaz de radio o bien una unidad emisora y receptora dentro del nodo de red. Puesto que esta unidad emisora y receptora consume relativamente mucha energía, pueden lograrse grandes ahorros de energía y/o un aumento significativo de la vida útil cuando también la unidad emisora y receptora se traslada a un modo de funcionamiento de reposo o bien se desactiva. Una desactivación de la unidad emisora y receptora limita por supuesto la posibilidad de alcanzar el correspondiente nodo de red y/o la comunicación con el mismo. También pueden trasladarse otros componentes, como por ejemplo una unidad de procesamiento (microprocesador), a un modo de reposo que ahorra energía.

Para hacer posible la desactivación de la unidad emisora y receptora o bien del módulo de radio de un nodo de red inalámbrico y a la vez asegurar que el mismo es alcanzable o asegurar una comunicación inalámbrica con el nodo de red, se dota por lo tanto tradicionalmente un nodo de red inalámbrico de una unidad emisora y receptora o componente receptor adicional, que solamente se prevé para activar el correspondiente nodo de red desde su estado de reposo o bien trasladarlo de un modo de servicio de reposo a un modo de servicio normal de trabajo. Este componente adicional emisor y receptor se denomina también Wake-Up-Radio o bien interfaz de activación. Para comunicar con el nodo de red envía entonces un emisor, que se encuentra por ejemplo en otro nodo de red, una señal de activación o bien una señal de wake-up al componente emisor y receptor de wake-up del nodo de red a activar, trasladándose el nodo de red receptor a activar mediante la señal de wake-up o bien señal de activación del modo de servicio de reposo a un modo de servicio normal de trabajo o conectándose. Tan pronto como el nodo de red se encuentra en el modo de servicio normal de trabajo, puede transmitir el emisor a los nodos de red el mensaje deseado, que es recibido por el equipo emisor y receptor activado previsto para ello o bien el módulo de radio del nodo de red. El componente Wake-Up-Radio o el componente adicional emisor y receptor previsto para la señal de activación está entonces diseñado tal que el mismo consume claramente menos energía que la unidad principal emisora y receptora usual para recibir mensajes.

Este modo de proceder tradicional para activar un nodo de red mediante una señal de activación o bien una señal de wake-up permite desde luego una posibilidad de ataque por parte de un tercero sobre el nodo de red o la red inalámbrica. Un atacante puede desde luego agotar en un tiempo relativamente corto la limitada energía almacenada en los nodos de red operados por batería de la red inalámbrica, activando los nodos de red desde el modo de servicio de reposo mediante envío continuo de una señal de activación y trasladándolo al modo de servicio normal. Un tal ataque se denomina también ataque Sleep Deprivation (privación de sueño).

Por el documento US 6,493,824 B1 se conoce un procedimiento para activar con seguridad una computadora mediante una tarjeta de red de la computadora en la que se recibe de una red un paquete de datos, se compara una dirección de destino contenida en el paquete de datos con una dirección de destino de la tarjeta de red y se busca dentro del paquete de datos un patrón de activación. En el caso de que las direcciones de destino coincidan y se encuentre un patrón de activación, se decodifica un valor codificado del paquete de datos y se compara con un valor esperado. Si coinciden los valores, se genera una señal para activar la computadora

Por el documento US 2005/0138377 A1 se conoce un procedimiento para autentificar y comunicar con seguridad en el que un aparato terminal de usuario que es activado desde el modo de servicio de reposo mediante algo diferente a una entrada de usuario, por ejemplo mediante una señal de activación, envía

sobre demanda de un servidor datos de máquina (machine credentials) para la autentificación al servidor. Sólo tras una autentificación con éxito se permite una comunicación con el aparato terminal del usuario.

Por el documento US 2006/0112287 A1 se conoce un procedimiento para activar inalámbricamente una computadora a través de una red de computadoras en la que a través de la red se difunde una señal con al menos una secuencia de datos de activación específica del aparato. Al respecto contiene cada secuencia de datos de activación varias iteraciones de la dirección de hardware de la tarjeta de red inalámbrica del correspondiente aparato. Durante el modo de reposo vigila la tarjeta de red los canales inalámbricos en cuanto a la presencia de paquetes de datos con secuencias de datos de activación. Si se recibe una secuencia de datos de activación, se compara la misma con la información de dirección de hardware de la tarjeta de red. Si hay coincidencia se activa el aparato.

Por el documento WO 00/33598 se conoce un procedimiento para la activación inalámbrica de una estación móvil en una red de telecomunicación inalámbrica, en el que se utiliza un procedimiento Challenge-Response (demanda-respuesta), para permitir una activación sólo mediante abonados de red autorizados.

Por el documento JP 2008283460 A se conoce un procedimiento para la comunicación de datos inalámbrica, en el que un nodo emisor, en base a una dirección de red de un nodo de destino, calcula informaciones multiplex del nodo de destino y transmite una señal de activación en base a las informaciones calculadas al nodo de destino, para hacer posible una recepción de datos por parte del nodo de destino. El nodo de destino se conecta entonces a un modo activo, en el que es posible una recepción de datos, cuando la señal de activación recibida coincide con informaciones multiplex propias del nodo de destino.

Es por lo tanto un objetivo de la presente invención lograr un procedimiento para la activación segura de un nodo de red a activar dentro de una red inalámbrica, que protege de un ataque de Sleep Deprivation.

Este objetivo se logra en el marco de la invención mediante un procedimiento con las características indicadas en la reivindicación 1.

La invención logra un procedimiento para activar un nodo de red de destino a activar de una red inalámbrica en el que el nodo de red de destino se activa desde un modo de servicio de reposo cuando un circuito de activación integrado del nodo de red recibe un token de activación secreto y lo verifica mediante una función de comprobación predeterminada y al menos un valor de referencia del token de activación memorizado, incluyendo la activación del nodo de red de destino (SN) una activación de un módulo principal de radio (2F) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

Para activar el nodo de red se utiliza así en el procedimiento correspondiente a la invención un token de activación secreto (Wake-Up-Token: WUT), en lugar de una señal fija conocida de wake-up o bien de activación, que se recibe a través de un módulo de radio de wake-up (Wake-Up-Radio). El token de activación secreto (WUT) es conocido entonces preferiblemente sólo por unidades emisoras y receptoras legítimas o bien autentificadas.

En una forma de ejecución del procedimiento correspondiente a la invención genera el propio nodo de red de destino el token de activación secreto y el valor de referencia del token de activación y antes de cambiar el nodo de red de destino al modo de servicio de reposo, se transmite a otro nodo de red de la red y por ejemplo allí se memorizan para la posterior activación del nodo de red de destino.

En una forma de ejecución alternativa del procedimiento correspondiente a la invención genera el token de activación y el valor de referencia del token de activación otro nodo de red de la red, transmitiéndose el valor de referencia del token de activación antes de cambiar el nodo de red de destino al modo de servicio de reposo al nodo de red de destino y memorizándose allí para la posterior activación del nodo de red de destino.

En una forma de ejecución posible del procedimiento correspondiente a la invención se generan el token de activación y el valor de referencia del token de activación mediante un nodo central de gestión de seguridad, una unidad de gestión de seguridad, un componente o por ejemplo un servidor.

En esta forma de ejecución existe dentro o fuera al menos un nodo de gestión o bien un nodo de gestión de seguridad SM (Security Manager) en la red inalámbrica. Esta forma de ejecución facilita la gestión y control de los token de activación y valores de referencia de los token de activación para los diversos nodos de red dentro de la red inalámbrica. El nodo de gestión de seguridad SM un puede ser un nodo separado autónomo. Alternativamente pueden estar implementadas funciones de gestión de seguridad en otro nodo, por ejemplo en un nodo de gateway (pasarela).

En una forma de ejecución del procedimiento correspondiente a la invención se transmite el valor de referencia del token de activación desde el nodo central de gestión de seguridad SM al correspondiente nodo de red de destino y antes de un cambio del nodo de red de destino al modo de servicio de reposo, se memoriza en el nodo de red de destino.

Al respecto proporciona el token de activación generado con preferencia el nodo central de gestión de seguridad a otro nodo de red para activar el nodo de red de destino.

En una forma de ejecución del procedimiento correspondiente a la invención genera el valor de referencia del token de activación el nodo de red de destino y el token de activación otro nodo de red de la red inalámbrica en base a la clave secreta común.

En una forma de ejecución del procedimiento correspondiente a la invención, se forman al respecto el valor de referencia del token de activación y el token de activación mediante una función de deducción de clave a partir de la correspondiente clave.

En una forma de ejecución posible del procedimiento correspondiente a la invención la función de deducción de clave es una función hash.

En una forma de ejecución posible del procedimiento correspondiente a la invención se renuevan el token de activación y el valor de referencia del token de activación tras cada proceso de activación del nodo de red de destino.

En otra forma de ejecución del procedimiento correspondiente a la invención se renuevan el token de activación y el valor de referencia del token de activación tras una cantidad predeterminada de procesos de activación del nodo de red de destino.

En otra forma de ejecución del procedimiento correspondiente a la invención se renuevan el token de activación y el valor de referencia del token de activación a intervalos de tiempo predeterminados.

En una forma de ejecución posible del procedimiento correspondiente a la invención se forman el token de activación y el valor de referencia del token de activación memorizado mediante dos miembros contiguos de una cadena hash compuesta por valores hash.

En una forma de ejecución del procedimiento correspondiente a la invención, se deducen el token de activación y el valor de referencia del token de activación de una cadena de caracteres. Al respecto puede componerse la cadena de caracteres del token de activación a partir de una o varias secuencias de caracteres.

En una forma de ejecución posible del procedimiento correspondiente a la invención presenta la secuencia de caracteres que puede componerse un código de identificación para identificar aquel nodo de red que envía el token de activación al nodo de red para activarlo.

En una forma de ejecución posible del procedimiento correspondiente a la invención presenta la secuencia de caracteres que puede componerse un Reason Code (código de motivo), que indica una razón para activar el nodo de red de destino.

En una forma de ejecución posible del procedimiento correspondiente a la invención presenta la secuencia de caracteres que puede componerse un código de activación condicional, que indica una condición para la activación del nodo de red de destino, activándose el nodo de red de destino cuando se cumple la condición. La condición se comprueba con preferencia mediante un componente de estructura del nodo de red de destino.

En una forma de ejecución posible del procedimiento correspondiente a la invención presenta la secuencia de caracteres que puede componerse una dirección de nodo correspondiente al nodo de red de destino.

En una forma de ejecución posible del procedimiento correspondiente a la invención presenta la secuencia de caracteres que puede componerse un código de activación predeterminado.

La invención logra además un nodo de red para una red inalámbrica con un circuito de activación integrado para trasladar el nodo de red desde un modo de servicio de reposo a un modo normal de servicio de trabajo, cuando el circuito de activación recibe un token de activación secreto y lo verifica mediante una función de comprobación predeterminada y mediante al menos un valor de referencia del token de activación memorizado, incluyendo el traslado del nodo de red al modo normal de servicio de trabajo (SN) una activación de un módulo principal de radio (2G) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

En una forma de ejecución del nodo de red correspondiente a la invención presenta el nodo de red una memoria para memorizar el valor de referencia del token de activación.

En una forma de ejecución del nodo de red correspondiente a la invención presenta el nodo de red un nodo de red de sensor con al menos un sensor.

En otra forma de ejecución de nodo de red correspondiente a la invención se forma el nodo de red mediante un aparato terminal de telecomunicación portátil.

Este aparato terminal de telecomunicación puede ser un teléfono móvil, un laptop o una PDA.

La invención logra además una red inalámbrica con varios nodos de red que presentan respectivos circuitos integrados de activación, que trasladan el correspondiente nodo de red desde un modo de servicio de reposo hasta un modo normal de servicio de trabajo cuando un token de activación secreto recibido es verificado mediante una función de comprobación predeterminada y al menos un valor de referencia del token de activación, incluyendo el traslado del nodo de red de destino al modo normal de servicio de trabajo (SN) una activación de un módulo principal de radio (2G) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

La invención logra además un programa de computadora con órdenes de programa para realizar un procedimiento para activar un nodo de red de destino a activar de una red inalámbrica, cuando se ejecuta el programa de computadora, activándose el nodo de red de destino desde un modo de servicio de reposo, en el caso de que el nodo de red de destino verifique un token de activación secreto recibido mediante una función de comprobación predeterminada y al menos un valor de referencia del token de activación memorizado, incluyendo la activación del nodo de red de destino (SN) una activación de un módulo principal de radio (2G) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

La invención logra además un soporte de datos que memoriza un tal programa de computadora.

Por lo demás, se describirán detalladamente formas de ejecución del procedimiento correspondiente a la invención del nodo de red correspondiente a la invención y de una red inalámbrica según la invención, con referencia a las figuras adjuntas.

Se muestra en:

figura 1 una red inalámbrica compuesta por nodos de red de sensor como ejemplo de ejecución de una red inalámbrica correspondiente a la invención, en la que se utiliza el procedimiento correspondiente a la invención para activar nodos de red;

figura 2 un diagrama para representar la comunicación entre dos nodos de red de sensor de la red de nodos de red de sensores representada en la figura 1, en la que un nodo de red es activado por otro nodo de red desde un modo de servicio de reposo;

figura 3 un esquema de bloques de circuitos de una forma de ejecución posible de un nodo de red según la invención;

figura 4 un diagrama secuencial para representar un ejemplo de ejecución del procedimiento correspondiente a la invención para activar un nodo de red;

figura 5 un diagrama de señales para representar un ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 6 otro diagrama de señales para representar un ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 7 un diagrama de señales para representar otro ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 8 un diagrama de señales para representar otro ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 9 un diagrama de señales para representar otro ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 10 un diagrama de señales para representar otro ejemplo de ejecución del procedimiento correspondiente a la invención;

figura 11 un diagrama de señales para representar otro ejemplo de ejecución del procedimiento correspondiente a la invención.

A continuación se describirán formas de ejecución del procedimiento correspondiente a la invención para activar un nodo de red dentro de una red inalámbrica y un nodo de red según la invención con referencia a las figuras adjuntas.

Tal como puede verse en la figura 1, en el ejemplo de ejecución representado está compuesta una red inalámbrica 1 por varios nodos de red 2, siendo una parte de los nodos, es decir, los nodos 2-1 a 2-4, nodos de red de sensor y el nodo 2-5 un nodo de pasarela (gateway), que conecta la red de sensores 1 con una red de infraestructura, por ejemplo Internet. El nodo de gateway 2-5 puede constituir un nodo central de gestión de seguridad o estar conectado con un nodo de gestión de seguridad separado. En una variante puede estar formado el nodo de gestión de seguridad por un nodo de red de sensor S.

Los nodos de red 2 de la red 1 correspondiente a la invención pueden ser nodos de red móviles, pero también nodos de red fijos.

Los nodos de red 2 de la red 1 comunican entre sí a través de una interfaz de radio inalámbrica. Los nodos de red 2 pueden conmutar entre distintos modos de servicio. En una posible forma de ejecución de la red correspondiente a la invención presentan los nodos de red 2 dos modos de servicio, que son un modo de servicio de reposo y un modo normal de servicio de trabajo. En el modo de servicio de reposo consume el correspondiente nodo de red 2 menos energía, para alargar lo más posible su vida útil o tiempo de funcionamiento debido a un posiblemente limitado el suministro por batería. En el modo normal de servicio de trabajo tiene el correspondiente nodo de red 2 su funcionalidad completa y puede por ejemplo transmitir datos de sensor captados al nodo de gateway 2-5 y desde allí a una unidad de procesamiento de datos.

La figura 2 muestra la activación de un nodo de red dentro de la red inalámbrica 1 mediante otro nodo de red. En el ejemplo representado se activa un nodo de red 2-2 mediante otro nodo de red 2-1, es decir, el nodo de red 2-2 se traslada desde un modo de servicio de reposo hasta un modo de servicio normal. El nodo de red 2-2 a activar mediante el nodo de red 2-1 se denomina también nodo de red de destino. Tal como se representa en la figura 2, envía el nodo de red 2-1 un token de activación secreto WUT (Wake-Up-Token) al nodo de red de destino 2-2. Este token de activación secreto WUT recibido se verifica dentro del nodo de red de destino 2-2 de recepción mediante una función de comprobación predeterminada y mediante al menos un valor de referencia del token de activación WUTRV (Wake-Up-Token-Reference-Value) memorizado. El wake-up-token WUT sólo es conocido por nodos emisores y receptores legitimados dentro de la red 1. El nodo de red de destino recibido comprueba el wake-up-token WUT mediante un valor de referencia del token de activación WUTRV. Si el wake-up-token WUT del nodo de red de destino 2-2 es recibido mediante su módulo wake-up de radio por el otro nodo de red 2-1, se activa el nodo de red de destino 2-2 desde un modo de servicio de reposo (Deep Sleep Mode). El conocimiento de un wake-up-token WUT autoriza así a un nodo de red 2-i de la red 1 para “despertar” o activar otro nodo de red 2-j dentro de la red 1.

A lo más tardar cuando un nodo de red 2 dentro de una red, debido a cualquier condición, cambia de su modo normal de servicio activo al modo de servicio de reposo, proporciona el mismo antes de la conmutación o bien del cambio de modo de servicio a otro componente o bien a otro nodo de red dentro de la red 1 uno o más tokens de activación WUT, archivándose una información de comprobación o bien un valor de referencia del token de activación WURTV para comprobar un wake-up-token WUT recibido en una memoria para el posterior proceso de activación.

La figura 3 muestra un diagrama de bloques de un ejemplo de ejecución de un nodo de red 2 correspondiente a la invención dentro de la red inalámbrica 1. En el ejemplo de ejecución representado en la figura 3 es un nodo de red de sensor, que está conectado mediante una unidad de entrada/salida (input/output) 2A o bien mediante una interfaz con uno o varios sensores 3, 3-1, 3-2. Los sensores 3-1, 3-2 pueden estar contenidos dentro del nodo de red del sensor 2 o bien estar integrados allí o bien conectados inalámbricamente o por línea física con la interfaz 2A. Los sensores pueden ser por ejemplo un sensor de temperatura, un sensor de humedad o un sensor de luminosidad. El nodo de red 2, tal como se representa en la figura 3, dispone de una unidad de procesamiento de datos o bien CPU 2B, que en la forma de ejecución representada tiene acceso a una memoria de datos flash 2C y a una memoria RAM 2D. En la memoria RAM 2D pueden estar memorizados transitoriamente por ejemplo datos de sensor aportados por los sensores 3-1, 3-2. Además puede presentar el nodo de red del sensor 2 una unidad de procesamiento de señales 2E. Tal como se representa en la figura 3, dispone de nodo de red 2 además de una unidad emisora y receptora o bien de un módulo principal de radio 2F, así como de un circuito integrado de activación 2G, que traslada o conmuta el nodo de red 2 tras recibir un token de activación secreto WUT, que se verifica mediante una función de comprobación predeterminada y un valor de referencia del token de activación WUTRV memorizado, desde un modo de servicio de reposo hasta un modo normal de servicio de trabajo.

En una forma de ejecución posible presenta el circuito integrado de activación 2G una memoria interna o bien un registro de datos en el que está memorizado el valor de referencia del token de activación WUTRV. La verificación mediante la función de comprobación se realiza mediante el circuito integrado de activación 2G del nodo de red de sensor 2. Las funciones del modo normal de servicio de trabajo se ejecutan por lo general mediante la CPU 2B del nodo de red 2. Contrariamente a la CPU 2B y al módulo emisor y receptor o bien el módulo principal de radio 2F, se caracteriza el circuito integrado de activación

2G del nodo de red 2 por un reducido consumo de energía. En una forma de ejecución posible se realiza la alimentación eléctrica del nodo de red 2 mediante una batería 2H allí prevista. Son posibles muchas variantes de ejecución diversas de un nodo de red 2 correspondiente a la invención. El ejemplo de ejecución representado en la figura 3 es un nodo de red de sensor para una red de sensores.

En una forma de ejecución alternativa el nodo de red 2 es también un aparato de telecomunicación portátil, por ejemplo un teléfono móvil, un laptop o una PDA.

Además es posible que el nodo de red 2 disponga, además de sensores, tal como se representa en la figura 3, también de actuadores, que se controlan mediante el nodo de red 2. Mediante un actuador puede por ejemplo abrirse o cerrarse una válvula. El nodo de red 2 es por lo general un nodo de red móvil, que por ejemplo opera mediante batería. Pero también es posible que el nodo de red 2 esté montado o depositado en un lugar de emplazamiento fijo y se alimente eléctricamente de otra manera, por ejemplo mediante una célula solar o similar.

La figura 4 muestra un diagrama secuencial para representar un ejemplo de ejecución del procedimiento correspondiente a la invención para activar un nodo de red de destino 2 a activar dentro de una red inalámbrica 1.

Tras una etapa de arranque S0, recibe el nodo de red 2 a activar primeramente en una etapa S1 un valor de referencia del token de activación WUTRV generado por otro componente o bien token y memoriza ese valor en una etapa S2 en una memoria de datos, por ejemplo en un registro de datos del circuito de activación 2G representado en la figura 3. Tras la memorización del valor de referencia del token de activación WUTRV en la etapa S2 puede cambiar el nodo de red 2 al modo de servicio de reposo que ahorra energía.

Tan pronto como el nodo de red de destino 2 recibe en la etapa S3 mediante el circuito integrado de activación 2G un token de activación WUT, comprueba el mismo este token de activación WUT recibido en la etapa S4 mediante una función de comprobación predeterminada y mediante el valor de referencia del token de activación WUTRV memorizado en la etapa S2. En el caso de que en la etapa S5 el token de activación WUT recibido se verifique mediante el circuito integrado de activación 2G, genera éste una señal de activación en la etapa S6, que activa los demás componentes y/o circuitos del nodo de red 2 desde el modo de servicio de reposo o los trasladan desde el modo de servicio de reposo hasta un modo normal de servicio de trabajo. Así se activa por ejemplo mediante la señal de activación generada en la etapa S6 la CPU 2B y el módulo principal de radio 2F para enviar y recibir mensajes. Tras la activación del nodo de red 2, finaliza el proceso de activación representado en la figura 4 en la etapa S7.

La verificación de un token de activación WUT recibido puede realizarse como sigue:

IF funciondecomprobacion (WUTRV, WUT) Returns TRUE THEN WAKE UP
(si la función de comprobación (WUTRV, WUT) da como resultado verdadero, entonces activar).

En una variante de ejecución se generan el token de activación WUT secreto y el valor de referencia del token de activación WUTRV mediante el propio nodo de red de destino. En este caso puede transmitir el nodo de red el token de activación formado antes de su cambio al modo de servicio de reposo a otro nodo de red de la red 1, que memoriza el token de activación WUT recibido para la posterior activación del nodo de red de destino.

En una forma de ejecución alternativa del procedimiento correspondiente a la invención, se generan el token de activación WUT y el valor de referencia del token de activación WUTRV mediante otro nodo de red de la red 1. En esta variante de ejecución se transmite el valor de referencia del token de activación WUTRV antes de un cambio del nodo de red de destino 2 al modo de servicio de reposo a este nodo de red de destino y se memoriza allí para la posterior activación del nodo de red de destino por ejemplo en un registro de datos del circuito de activación 2G allí integrado.

En una variante de ejecución se genera para un token de activación el correspondiente valor de referencia del token de activación WUTRV mediante un nodo central de gestión de seguridad, por ejemplo en el ejemplo representado en la figura 1 mediante un nodo de gateway 2-5. El valor de referencia del token de activación WUTRV generado se transmite a continuación desde el nodo central de gestión de seguridad 2-5 al nodo de red de destino 2-i y antes de cambiar el nodo de red de destino al modo de servicio de reposo, se memoriza en este nodo de red de destino 2-i para el posterior proceso de activación. El token de activación generado por el nodo central de gestión de seguridad 2-5 puede entonces proporcionarse a otro nodo de red dentro de la red 1 para activar el nodo de red de destino.

De esta manera puede solicitar un nodo de red 2 que desea activar el nodo de red de destino que se encuentra en reposo el wake-up-token WUT necesario para ello directamente del nodo central de gestión de seguridad 2-5.

En una posible variante de ejecución proporciona el nodo de gestión de seguridad 2-5 al nodo 2 que realiza la demanda el token de activación WUT solicitado sólo tras la correspondiente comprobación de autorización.

En una forma de ejecución posible del procedimiento correspondiente a la invención se generan en valor de referencia del token de activación WUTRV y el token de activación WUT separadamente mediante diversos nodos de red 2 de la red inalámbrica 1 en base a una clave secreta común K. Por ejemplo puede generarse el valor de referencia del token de activación WUTRV mediante el nodo de red de destino a activar y el token de activación WUT mediante otro nodo de red que desea activar el nodo de red de destino en base a una clave secreta común K.

En una forma de ejecución posible pueden formarse entonces el valor de referencia del token de activación WUTRV y el token de activación WUT mediante una función de deducción de clave KDF (Key Derivation Function) a partir de la clave K.

$$WUT = KDF(K)$$

En una variante de ejecución posible la función de deducción de clave KDF utilizada es una función hash.

En una forma de ejecución posible se utiliza una clave criptográfica K existente de todos modos para otra finalidad. Por ejemplo puede utilizarse una clave conocida en toda la red, una llamada Network Key.

Como función de deducción de clave KDF puede utilizarse por ejemplo una función hash de clave (Key-Hash-Function) como por ejemplo HMAC-SHA1, que adicionalmente utiliza una cadena de caracteres fija como parámetro de entrada.

En una forma de ejecución posible del procedimiento correspondiente a la invención se deducen el token de activación WUT y el valor de referencia del token de activación WUTRV de una cadena de caracteres que puede componerse. Esta cadena de caracteres que puede componerse puede componerse a partir de una o varias secuencias de caracteres. Estas secuencias de caracteres que pueden componerse pueden codificar diversas informaciones.

En una forma de ejecución posible presenta la secuencia de caracteres que puede componerse un código de identificación IC, que sirve para identificar aquel nodo de red 2 dentro de la red 1 que envía el token de activación WUT al nodo de red de destino para activarlo. De esta manera contiene el token de activación WUT una información sobre el nodo emisor. Para recibir un tal token de activación WUT mediante el circuito de activación 2G integrado del nodo de red a activar 2, puede detectar el nodo de red 2 directamente tras su activación o bien tras la conexión al modo normal de servicio la identidad de aquel nodo de red que le ha activado. De esta manera puede decidir el nodo de red 2 activado, o el nodo de red de destino entre otros, de qué nodo de red tomará el mismo los mensajes recibidos a continuación. Además hace posible en cierta medida el prever un código de identificación IC una llamada de retorno en la que el nodo de red 2 activado toma contacto con el nodo de red que realiza la activación.

En otra variante de ejecución presenta la secuencia de caracteres que puede componerse correspondiente a la cadena de caracteres de la que pueden deducirse el token de activación y el valor de referencia del token de activación, un llamado Reason-Code RC, que indica la razón por la que se activa el nodo de red de destino 2. El Reason-Code o código de argumentación RC indica entonces por qué debe activarse el nodo de red 2. Posibles razones para activar un nodo de red 2 pueden ser por ejemplo la retrasmisión de paquetes de datos o de paquetes de datos de alarmas o la necesaria determinación de valores de sensor o la realización de tareas de configuración. El Reason-Code o bien código de argumentación RC y el token de activación WUT pueden estar configurados tal que el circuito integrado de activación 2G del nodo de red 2 a activar puede decidir ya al recibir cada bit individual si la parte restante del token de activación WUT o bien del Reason-Code RC es relevante para el nodo de red 2 a activar que realiza la recepción o si puede ignorarse.

Basándose en el Reason-Code RC recibido, puede así decidir el circuito de activación o bien el componente Wake-Up-Radio 2G del nodo de red de destino 2 que realiza la recepción si el nodo de red 2 se activará o no desde el modo de servicio de reposo. La información de por qué ha de trasladarse el nodo de red de destino 2 desde el modo de servicio de reposo al modo de servicio normal, queda disponible para el nodo de red de destino 2 directamente una vez activado y puede tenerse en cuenta para el posterior procesamiento de los datos.

Además es posible que el nodo de red de destino 2 activado comunique al componente Wake-Up-Radio o bien al circuito integrado de activación 2G antes de una transición al modo de servicio de reposo, que él sólo debe activarse para Reason-Codes RC o códigos de argumentación RC predeterminados. De esta

manera es posible, entre otros, un comportamiento del nodo de red de destino 2 adaptado al estado actual en cuanto a energía del nodo de red de destino 2.

En otra forma de ejecución del procedimiento correspondiente a la invención presenta una secuencia de caracteres que puede componerse una cadena de caracteres en base a la cual pueden formarse el token de activación WUT y el valor de referencia del token de activación WUTRV, un código de activación condicional o un Conditional-Wake-Up-Code.

El código de activación condicional indica una condición para la activación del nodo de red de destino 2. El código de activación Conditional o de condiciones puede indicar por ejemplo al circuito integrado de activación 2G del nodo de red de destino 2 que realice una medición mediante un sensor 3 del nodo de red de destino 2 y se traslade el nodo de red de destino 2 desde el modo de servicio de reposo al modo de servicio normal sólo si existe o se cumple una determinada condición. Una tal condición puede consistir por ejemplo en que el valor de medida aportado por el sensor 3 se encuentre por encima de un valor de umbral predeterminado. Una tal medición es posible con uno o con algunos sensores 3 sin participación de otros componentes del nodo de red de destino 2, con lo que el nodo de red de destino 2 puede seguir permaneciendo a continuación en el modo de servicio de reposo. Esta variante de ejecución ofrece la ventaja de que en el proceso antes citado la unidad principal y receptora o bien el módulo principal de radio 2F del nodo de red de destino 2 no tienen que activarse y con ello el consumo de corriente es mínimo. Además, tras activar el nodo de red de destino 2 se dispone ya de informaciones sobre la razón de la activación, así como de valores de medida de sensores, por lo que es posible un procesamiento inmediato de señales y datos.

En una forma de ejecución se transfiere por ejemplo un valor de sensor que aporta un sensor 3-1, 3-2 a través de la unidad de E/S 2A directamente al circuito de activación 2G. En una forma de ejecución se compara el valor del sensor o bien una señal de medida analógica mediante un comparador con un valor de referencia o comparativo. Esto puede realizarse tanto analógica como también digitalmente. La CPU 2B puede entonces activarse en función de la señal de salida del comparador y comprobar al menos una condición predeterminada. Si no se cumple esta condición, retorna la CPU 2B al modo de servicio de reposo. Pero si se cumple la condición, se activa mediante la CPU 2B el nodo de red completo, inclusive el módulo principal de radio 2F.

En una variante de ejecución está codificado en el código wake-up o el código de activación condicional qué condiciones han de comprobarse. Alternativamente pueden existir estas informaciones memorizadas como pertenecientes a un determinado wake-up-code.

Son posibles otras variantes de ejecución del procedimiento correspondiente a la invención. Por ejemplo puede presentar la secuencia de caracteres que puede componerse para una cadena de caracteres, sobre cuya base se deducen el token de activación WUT y el valor de referencia del token de activación WUTRV, una dirección de nodo del nodo de red de destino 2 o un wake-up-code o código de activación. Comparado con un wake-up-code fijo, ofrece este proceder una mejor protección frente a ataques, ya que un wake-up-code utilizado una vez no puede introducirse de nuevo con éxito.

La utilización del reason code o código de argumentación RC y código condicional o de activación o Conditional-Wake-Up-Codes posibilita a un nodo de red de destino 2 procesar sólo eventos y mensajes relevantes para el mismo. Esta decisión del nodo de red de destino 2 se toma mientras el nodo de red de destino 2 se encuentra aún en el modo de servicio de reposo que ahorra energía, con lo que puede lograrse una vida útil o tiempo de funcionamiento del correspondiente nodo de red de destino 2 claramente prolongados.

Mediante la utilización de wake-up-token WUT con o sin reason codes o wake-up-codes condicionales, dispone un nodo de red de destino 2 ya inmediatamente después de su activación de otras informaciones, por ejemplo de la identidad del nodo de red que realiza la activación, de la razón de la activación o de la condición que ha entrado de un valor de sensor. De esta manera quedan garantizados un procesamiento más rápido de mensajes y una reacción más rápida a eventos. Así se acelera en su conjunto el procesamiento de datos dentro de la red 1.

Para aumentar la seguridad puede renovarse en una variante de ejecución del procedimiento correspondiente a la invención el token de activación WUT y el valor de referencia del token de activación WUTRV de un nodo 2.

En una variante de ejecución se realiza una renovación del token de activación WUT y del correspondiente valor de referencia del token de activación WUTRV con cada proceso de activación del nodo de red de destino 2.

En otra variante de ejecución se realiza una renovación del token de activación WUT y del valor de referencia del token de activación WUTRV tras un número predeterminado de procesos de activación del nodo de red de destino 2.

En otra variante de ejecución se realiza la renovación del token de activación WUT y del correspondiente valor de referencia del token de activación WUTRV a intervalos de tiempo determinados, es decir, periódicamente.

En una variante de ejecución del procedimiento correspondiente a la invención se forman el valor de referencia del token de activación WUTRV y el token de activación WUT mediante una función de deducción de claves KDF a partir de una clave criptográfica secreta K. Esta clave K puede ser en una variante de ejecución una clave de red conocida de un valor de red.

En una forma de ejecución alternativa la clave criptográfica es una clave K que además de al nodo de red de destino 2 sólo le es conocida a un segundo nodo de red, es decir, existe en esta variante de ejecución una relación de seguridad entre estos dos nodos de red.

En otra variante de ejecución sólo conoce la clave criptográfica K un grupo predeterminado de nodos de red y constituye una clave de grupo.

En una forma de ejecución del procedimiento correspondiente a la invención la función de deducción de clave KDF es una función hash.

En una posible variante de ejecución se forman el token de activación WUT y el valor de referencia del token de activación WUTRV memorizado mediante dos miembros contiguos de una cadena hash compuesta por valores hash. Entonces se toman el valor de referencia del token de activación WUTRV y el token de activación WUT de una cadena hash que conocen tanto el nodo emisor como también el nodo receptor. En esta variante de ejecución se determina para la siguiente fase de reposo del nodo de red de destino 2 el wake-up-token en base al siguiente valor hash dentro de la tabla hash y/o de la cadena hash. Mediante esta forma de proceder queda asegurado que para cada proceso de activación se utiliza otro token de activación WUT que sólo conocen el nodo emisor y el nodo receptor.

Cuando ya se ha utilizado un token de activación (token antiguo), dado el caso puede conocerlo ya un atacante cuando ha realizado una escucha en la transmisión. Puede evitarse un tal ataque utilizando otro token de activación que no sea idéntico. En esta variante de ejecución es diferente un nuevo token de activación (token nuevo) del token de activación WUT (token antiguo) previamente utilizado. Un nuevo token de activación WUT_i puede calcularse a partir de un token WUT_{i-1} ya utilizado mediante una función hash criptográfica irreversible, como por ejemplo MD5, SHA-1 o SHA-56.

$$WUTi = H(WUT_{i-1})$$

Un tercero externo o un atacante no puede, incluso si conoce el token utilizado hasta ahora WUT_{i-1}, determinar con un coste asumible en cálculo un nuevo token WUTi adecuado.

En una posible variante de ejecución se calculan tanto el nodo de emisión como también el nodo de recepción y/o el nodo de red de destino 2 a partir de un token de valor de anclaje (Token Anchor) conocido mediante una secuencia de valores hash de una cadena hash:

$$Token1 = H(Token\ Anchor)$$

$$Token2 = H(Token1)...$$

$$Token(n) = H\ (Token(n-1))$$

Los token o bien valores hash se utilizan entonces para la verificación mediante los nodos de red 2 hacia atrás, comenzando con el token (n) seguido por el token (n-1) y así sucesivamente.

Una ventaja de esta variante de ejecución consiste en que en nodos de red -2, que a menudo se activan, no tiene que establecerse cada vez o bien en cada proceso de activación un nuevo wake-up-token WUT o bien un nuevo valor de referencia del token de activación WUTRV. Para esta variante de ejecución puede utilizarse un valor de token de activación o bien valor de referencia del token de activación establecido una sola vez, es decir, un valor de anclaje (Token Anchor) para n operaciones de activación.

Las figuras 5 a 11 muestran diagramas de señales para explicar diversas variantes de ejecución del procedimiento correspondiente a la invención para activar un nodo de red de destino 2.

La figura 5 muestra una variante de ejecución en la que el valor de referencia del token de activación (WUTRV) se realiza mediante el propio nodo de red de destino SN a activar. En la representación de la figura 5 designa SN el nodo de red de destino a activar (SN: Sleep Node) y WN el nodo que activa (WN: Wake-Up Node), el cual activa el nodo de red de destino SN a activar. La comunicación a través del canal de comunicación regular, es decir, a través del módulo principal de radio 2F representado en la figura 3, se representa en las siguientes figuras 5-11 como flecha sencilla y por el contrario una comunicación a través del Wake-Up-Radio o bien a través del circuito de activación 2G integrado, se representa como flecha gruesa discontinua.

Tal como se representa en la figura 5, genera (S5-1) el nodo de red de destino SN a activar primeramente por sí mismo el token de activación WUT secreto y el correspondiente valor de referencia del token de activación WUTRV, pudiendo memorizarse el valor de referencia del token de activación WUTRV en un registro del circuito integrado de activación 2G. A continuación transmite (S5-2) el nodo de red de destino SN a activar el token de activación WUT secreto para una posterior nueva activación a otro nodo de red 2 de la red 1, por ejemplo al nodo WN representado en la figura 5. Este nodo WN puede memorizar (S5-3) el token de activación WUT recibido en una memoria. Entonces puede memorizarse el token de activación WUT recibido del nodo de red de destino SN perteneciente a una dirección de destino del nodo de red de destino SN.

Tan pronto como el nodo de red de destino SN ha transmitido el token de activación WUT a al menos otro nodo de red dentro de la red 1, puede cambiar el mismo (S5-4) al modo de servicio de reposo.

Si detecta el otro nodo de red WN el cumplimiento de una condición de activación para el nodo de red de destino SN (SN-5), entonces transmite (SN-6) el mismo el token de activación WUT memorizado al Wake-Up-Radio o bien al circuito de activación 2G integrado del nodo de red de destino SN. El circuito de activación 2G integrado del nodo de red de destino SN realiza una comprobación del token de activación WUT recibido (S5-7). Entonces se verifica el token de activación WUT secreto recibido mediante una función de comprobación predeterminada y mediante al menos un valor de referencia del token de activación WUTRV memorizado. Si en el ejemplo representado en la figura 5 tiene éxito la verificación del token de activación WUT recibido, se traslada el nodo de red de destino SN desde el modo de servicio de reposo de hasta un modo normal de servicio de trabajo. En el ejemplo representado solicita el nodo de activación WN que ha activado el nodo de red de destino SN tras un tiempo determinado datos (S5-8), por ejemplo datos del sensor. Éstos son proporcionados (S5-9) por el nodo de red de destino SN activado, por ejemplo un nodo de red de sensor. Por ejemplo transmite el nodo de red de destino SN datos del sensor a través del canal de comunicación regular al nodo de activación WN.

La figura 6 representa una variante de ejecución en la que primeramente otro nodo de red WN2 envía (S6-5) otro wake-up-token WUT2 o bien uno defectuoso. En este caso permanece el nodo de red de destino SN primeramente en el modo de servicio de reposo. Sólo cuando el nodo WN que dispone del token de activación WUT correcto transmite (S6-7) este token de activación al nodo de red de destino, se activa (S6-8) el nodo de red de destino SN desde el modo de servicio de reposo, como se representa en la figura 6 y puede transmitir (S6-10) los datos al nodo de red WN que realiza la reactivación cuando se realiza la correspondiente solicitud (S6-9).

La figura 7 muestra una variante de ejecución en la que el valor de referencia del token de activación WUTRV se establece mediante un nodo de gestión de seguridad local o un nodo de gestión de seguridad SM. El nodo de gestión de seguridad SM genera (S7-1) tanto el token de activación WUT como también el correspondiente valor de referencia del token de activación WUTRV, poniendo el mismo el valor de referencia del token de activación WUTRV a disposición (S7-2) del nodo de red de destino SN, que memoriza el mismo (S7-3) y pone el correspondiente token de activación WUT depositado, para que quede almacenado, a disposición (S7-1) de otro nodo de red WN, que memoriza el mismo (S7-5). El nodo de red de destino SN cambia (S7-6) debido al mismo al modo de servicio de reposo. Tan pronto como el nodo de red WN detecta (S7-7) la introducción de una condición de activación, transmite el mismo (S7-8) en el ejemplo representado el token de activación WUT al Wake-Up-Radio del nodo de red de destino SN, que verifica el mismo como correcto (S7-9). A continuación puede realizarse (S7-11) la transmisión de los datos tras solicitarlo (S7-10) el nodo de red de destino SN al nodo de red que realiza la activación.

La figura 8 muestra otra variante de ejecución del procedimiento correspondiente a la invención en el que se establece igualmente el valor de referencia del token de activación WUTRV mediante un nodo de gestión de seguridad SM, proporcionando no obstante el token de activación WUT a este nodo WN un nodo de red WN de la red 1 solamente sobre demanda o bien cuando se necesita. Cuando en el ejemplo de ejecución representado en la figura 8 detecta un nodo de red WN la introducción de una condición de activación para el nodo de red de destino SN (S8-5), pregunta el mismo (S8-6) al nodo de gestión de seguridad SM si puede recibir un token de activación WUT adecuado para el nodo de red de destino SN. El nodo de gestión de seguridad SM comprueba (S8-7) en el ejemplo de ejecución representado en la figura 8 si el nodo de red SN que realiza la pregunta tiene el derecho de activar el nodo de red de destino

SN o no. En el ejemplo representado tiene el nodo de red WN que pregunta el derecho de activar el nodo de red de destino SN y recibe (S8-8) el token de activación WUT necesario para ello. Este token de activación WUT recibido lo transmite (S8-9) el nodo de red WN al circuito de activación 2G integrado del nodo de red de destino SN, que comprueba este token de activación WUT (S8-10). En el ejemplo representado tiene éxito la verificación del token de activación WUT recibido y el nodo de red de destino SN puede aportar (S8-12) los datos solicitados (S8-11) por el nodo WN.

La figura 9 representa otra variante de ejecución, en la que un token de activación WUT generado por el nodo de red de destino SN se registra en un nodo central de gestión de seguridad SM. En el caso de que un nodo de red WN, tras detectar (S9-6) una condición de activación para un nodo de red de destino SN, necesite un token de activación WUT adecuado, recibe el mismo (S9-9) sobre demanda (S9-7) el token de activación WUT registrado en el nodo de seguridad SM, siempre que el nodo de red que realiza la consulta WN, tras la comprobación (S9-8), resulte que está autorizado para activar el nodo de red de destino SN.

La figura 10 muestra otra variante de ejecución del procedimiento correspondiente a la invención, en la que el token de activación WUT generado está compuesto por valores hash calculados de una cadena hash. Un nodo WN de la red 1 calcula (S10-1) varios valores hash H_i de una cadena hash, por ejemplo basándose en un valor de anclaje. Un valor hash H_n de la cadena hash se transmite (S10-2) como token de activación WUT al nodo de red de destino SN y se verifica (S10-7) mediante un valor hash contiguo de la cadena hash, es decir, el valor hash H_{n-1}. Si la verificación tiene éxito, cambia el nodo de red de destino SN del modo de servicio de reposo al modo de servicio normal y transmite (S10-9) los datos solicitados (S10-8) al nodo de red WN.

La figura 11 muestra otra variante de ejecución en la que el token de activación WUT y el correspondiente valor de referencia del token de activación WUTRV se deducen separadamente (S11-1, S11-2) mediante un nodo de red WN de la red 1 y mediante el nodo de red de destino SN de una clave criptográfica K y se memorizan (S11-3, S11-4). Ambos nodos WN, SN pueden utilizar entonces las mismas o distintas funciones de deducción de claves KDF. Tras detectar (S11-6) una condición de activación el nodo WN (S11-5) se activa el nodo de destino SN trasladado al modo de servicio de reposo en la etapa S11-5 tras verificarse (S11-8) el WUT transmitido (S11-7) y proporciona (S11-10) los datos solicitados (S11-9).

Mediante la utilización de un token de activación WUT secreto, preferiblemente cambiante, se evita en el procedimiento correspondiente a la invención un ataque de Sleep Deprivation, en el que un atacante activa constantemente el nodo de red 2, para impedir a ese nodo de red 2 permanecer en un modo de servicio de reposo ahorrador de energía.

El procedimiento correspondiente a la invención impide así que se acorte la vida útil o el tiempo de funcionamiento de los nodos de red 2 debido a ataques de Sleep Deprivation. Mediante ataques de Sleep Deprivation puede reducirse el tiempo de funcionamiento de un nodo de red de sensor o de un nodo de red 2 de una red inalámbrica 1 de algunos años a algunas horas. La indeseada reducción de la vida útil se evita mediante la forma de proceder correspondiente a la invención.

REIVINDICACIONES

1. Procedimiento para activar un nodo de red de destino (SN) a activar de una red inalámbrica (1), en el que el nodo de red de destino (SN) se activa desde un modo de servicio de reposo cuando un circuito de activación integrado (2G) del nodo de red de destino (SN) recibe un token de activación (WUT) secreto y lo verifica mediante una función de comprobación predeterminada y al menos un valor de referencia del token de activación (WUTRV) memorizado, incluyendo la activación del nodo de red de destino (SN) una activación de un módulo principal de radio (2F) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

2. Procedimiento según la reivindicación 1, en el que el token de activación secreto (WUT) y el valor de referencia del token de activación (WUTRV) los genera el propio nodo de red de destino (SN) y antes de cambiar el nodo de red de destino (SN) al modo de servicio de reposo, se transmite a otro nodo de red (WN, SM) de la red (1) y allí se memorizan para la posterior activación del nodo de red de destino (SN).

3. Procedimiento según la reivindicación 1, en el que el token de activación (WUT) y el valor de referencia del token de activación (WUTRV) los genera otro nodo de red (SM, WN) de la red (1), transmitiéndose el valor de referencia del token de activación (WUTRV) antes de cambiar el nodo de red de destino (SN) en el modo de servicio de reposo al nodo de red de destino (NWK) y memorizándose allí para la posterior activación del nodo de red de destino (SN).

4. Procedimiento según la reivindicación 3, en el que el token de activación (WUT) y el valor de referencia del token de activación (WUTRV) se generan mediante un nodo central de gestión de seguridad (SM).

5. Procedimiento según la reivindicación 4, en el que se transmite el valor de referencia del token de activación (WUTRV) generado desde el nodo central de gestión de seguridad (SM) al nodo de red de destino (SN) y antes de un cambio del nodo de red de destino (SN) al modo de servicio de reposo, se memoriza en el nodo de red de destino (SN).

6. Procedimiento según la reivindicación 5, en el que el nodo central de gestión de seguridad (SM) proporciona el token de activación generado (WUT) a otro nodo de red (WN) para activar el nodo de red de destino (SN).

7. Procedimiento según la reivindicación 1, en el que se genera el valor de referencia del token de activación (WUTRV) mediante el nodo de red de destino (NWK) y el token de activación (WUT) mediante otro nodo de red (SM, WN) de la red inalámbrica (1) en base a una clave secreta común (K).

8. Procedimiento según la reivindicación 7, en el que el valor de referencia del token de activación (WUTRV) y el token de activación (WUT) se forman mediante una función de deducción de clave (KDF) a partir de la clave (K).

9. Procedimiento según la reivindicación 8, en el que la función de deducción de clave (KDF) es una función hash.

10. Procedimiento según una de las reivindicaciones 1-9, en el que se renuevan el token de activación (WUT) y el valor de referencia del token de activación (WUTRV) tras cada proceso de activación del nodo de red de destino (SN) o tras una cantidad predeterminada de procesos de activación del nodo de red de destino (SN) o a intervalos de tiempo predeterminados.

11. Procedimiento según la reivindicación 9, en el que el token de activación (WUT) y el valor de referencia del token de activación (WUTRV) memorizado se forman mediante dos miembros contiguos de una cadena hash compuesta por valores hash.

12. Procedimiento según una de las reivindicaciones 1-11, en el que el token de activación (WUT) y el valor de referencia del token de activación (WUTRV) se deducen de una cadena de caracteres.

13. Procedimiento según la reivindicación 12, en el que la cadena de caracteres del token de activación (WUT) se compone a partir de una o varias secuencias de caracteres.

14. Procedimiento según la reivindicación 13,
en el que la secuencia de caracteres que puede componerse presenta:
- un código de identificación (IC) para identificar aquel nodo de red que envía el token de activación (WUT) al nodo de red (NWK) para activarlo,
- un Reason Code (RC), que indica una razón para activar el nodo de red de destino (NWK),
- un código de activación condicional, que indica una condición para la activación del nodo de red de destino (NWK),
- una dirección de nodo del nodo de red de destino (NWK) o
- un código de activación predeterminado.

15. Nodo de red (2) para una red inalámbrica (1) con un circuito de activación integrado (2G) para trasladar el nodo de red (2) desde un modo de servicio de reposo a un modo normal de servicio de trabajo,
cuando el circuito de activación (2G) recibe un token de activación (WUT) secreto de recepción y lo verifica mediante una función de comprobación predeterminada y al menos un valor de referencia del token de activación (WUTRV) memorizado,
incluyendo el traslado del nodo de red al modo normal de servicio de trabajo (SN) una activación de un módulo principal de radio (2G) para enviar y recibir mensajes y teniendo el circuito de activación (2G) un consumo de energía inferior al del módulo principal de radio (2F).

16. Nodo de red según la reivindicación 15,
en el que el nodo de red (2) presenta una memoria para memorizar el valor de referencia del token de activación (WUTRV).

17. Nodo de red según una de las reivindicaciones 15 ó 16,
en el que el nodo de red (2) es un nodo de red de sensor con al menos un sensor (3).

18. Nodo de red según una de las reivindicaciones 15 ó 16,
en el que el nodo de red (2) es un aparato terminal de telecomunicación portátil.

19. Nodo de red según la reivindicación 18,
en el que el aparato terminal de telecomunicación es un teléfono móvil, un laptop o una PDA.

20. Red inalámbrica (1) con varios nodos de red (2) según una de las reivindicaciones precedentes 15-19.

21. Programa de computadora con órdenes de programa para realizar el procedimiento según una de las reivindicaciones 1-14 cuando se ejecuta el programa de computadora.

22. Soporte de datos que memoriza el programa de computadora según la reivindicación 21.

FIG 1

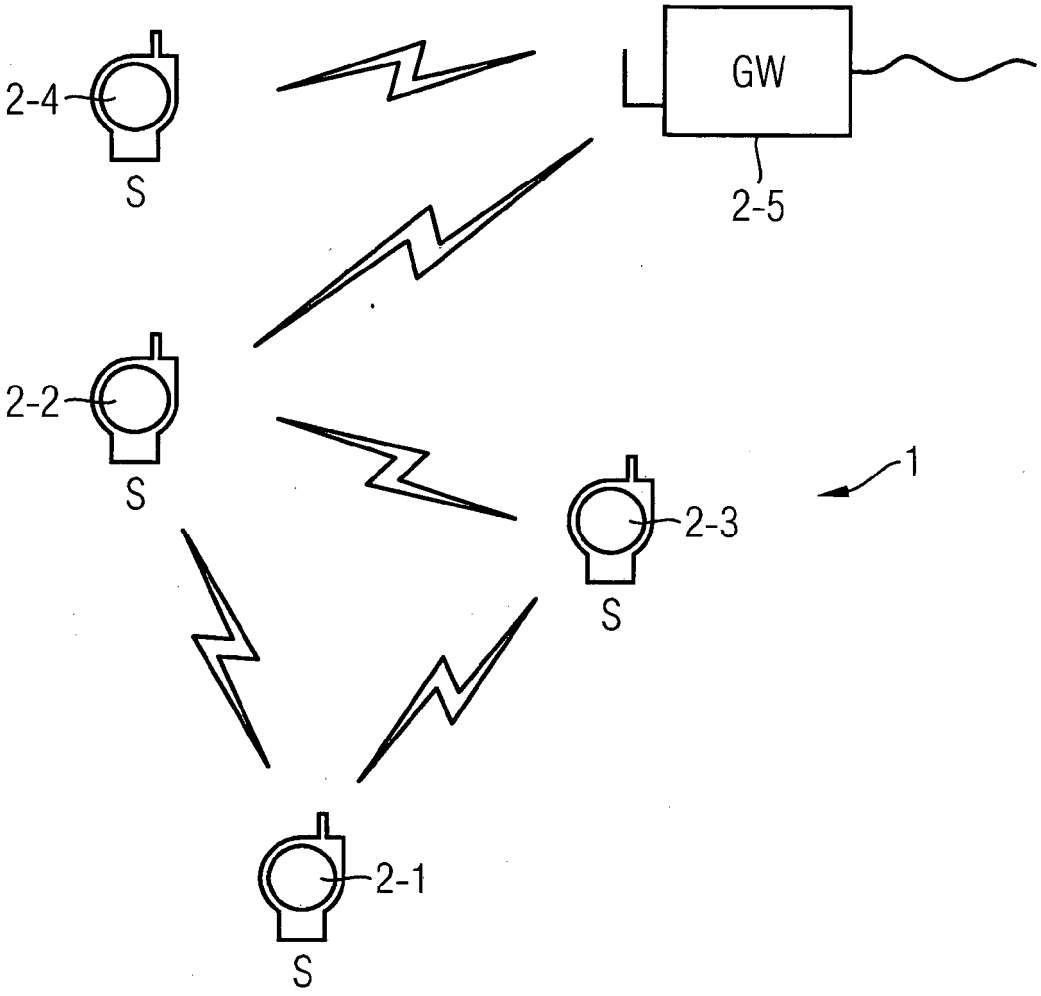


FIG 2

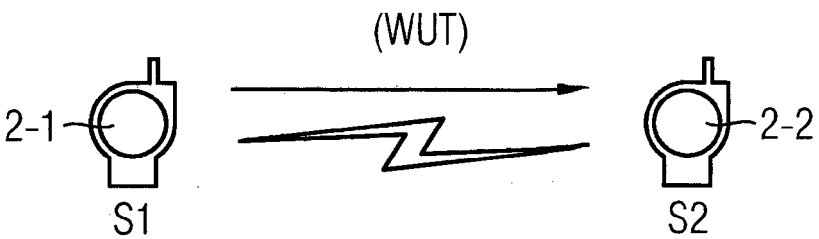


FIG 3

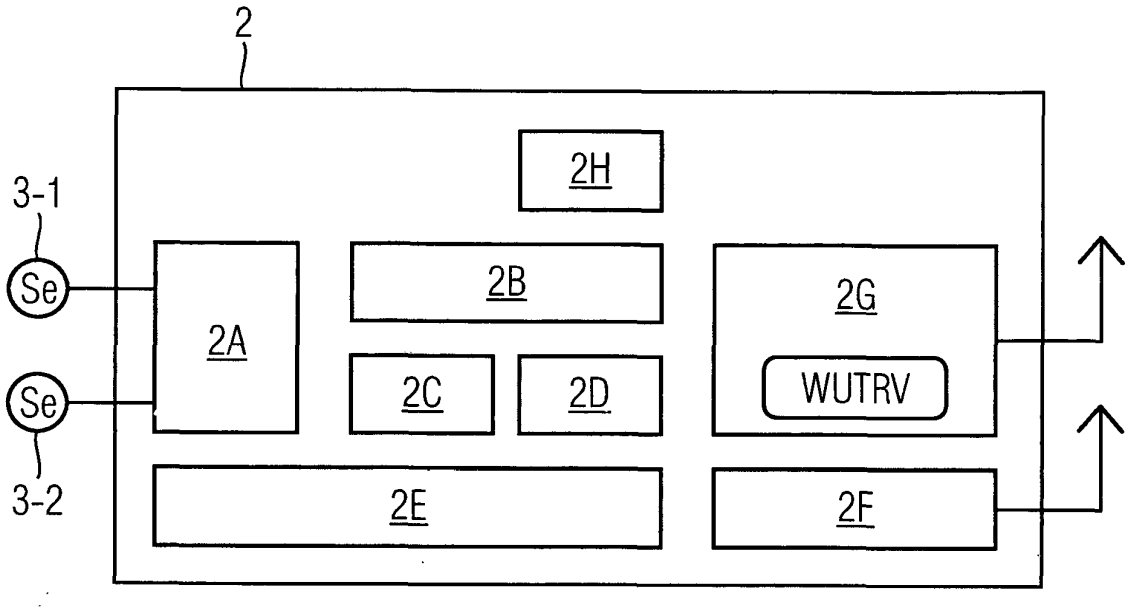


FIG 4

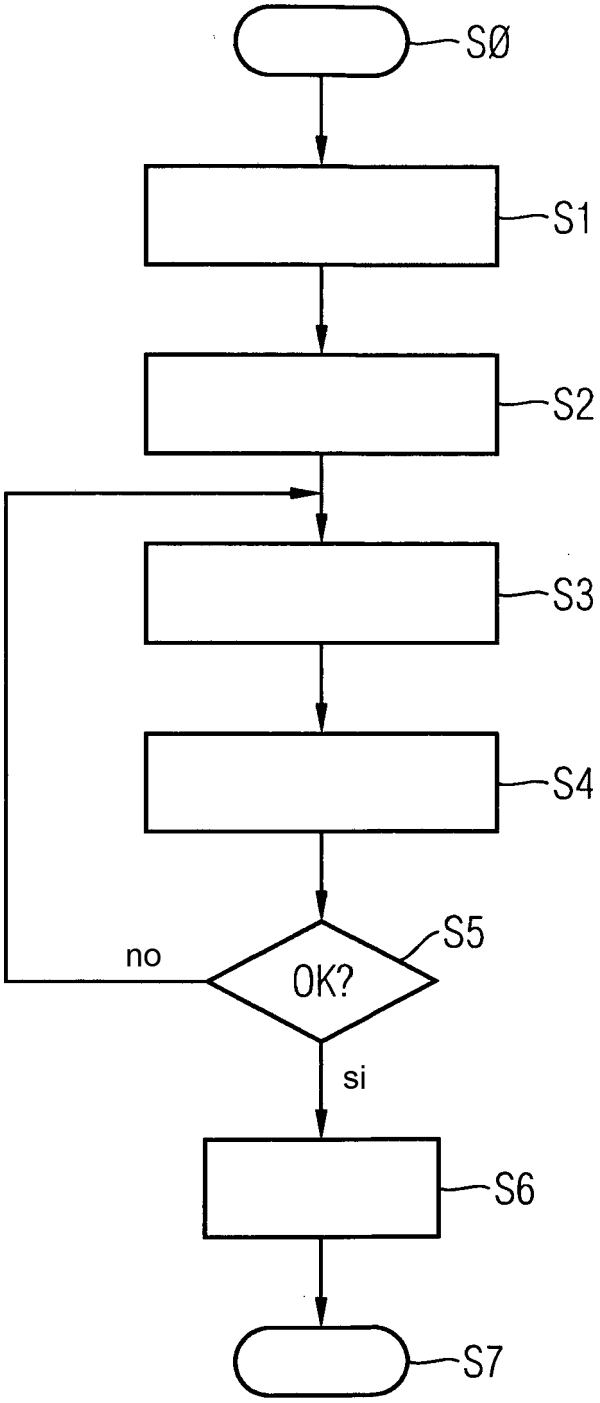


FIG 5

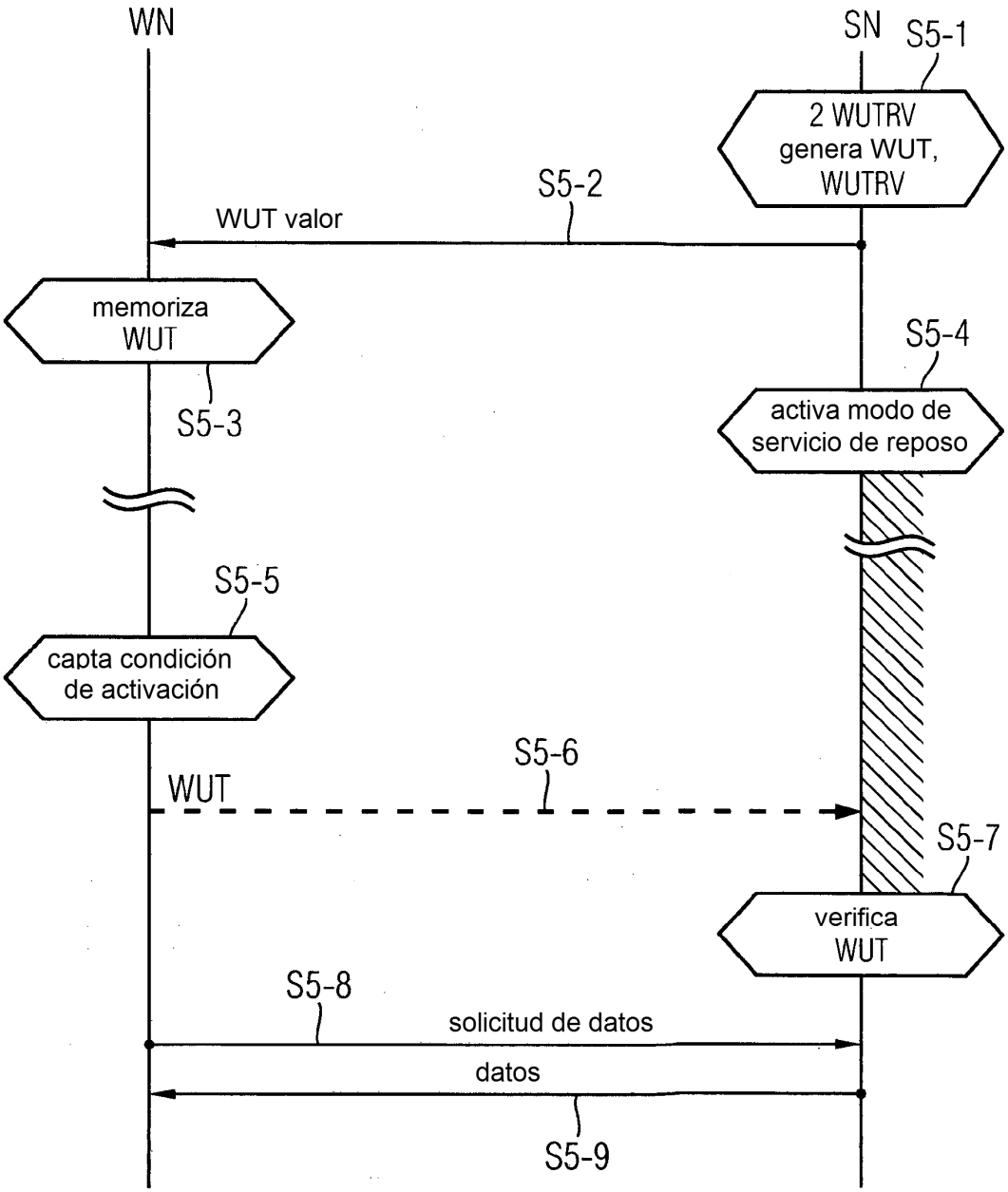

WN
SN
S5-1
2 WUTRV
genera WUT,
WUTRV
S5-2
WUT valor
memoriza
WUT
S5-3
S5-4
activa modo de
servicio de reposo
S5-5
capta condición
de activación
S5-6
WUT
S5-7
verifica
WUT
S5-8
solicitud de datos
datos
S5-9

FIG 6

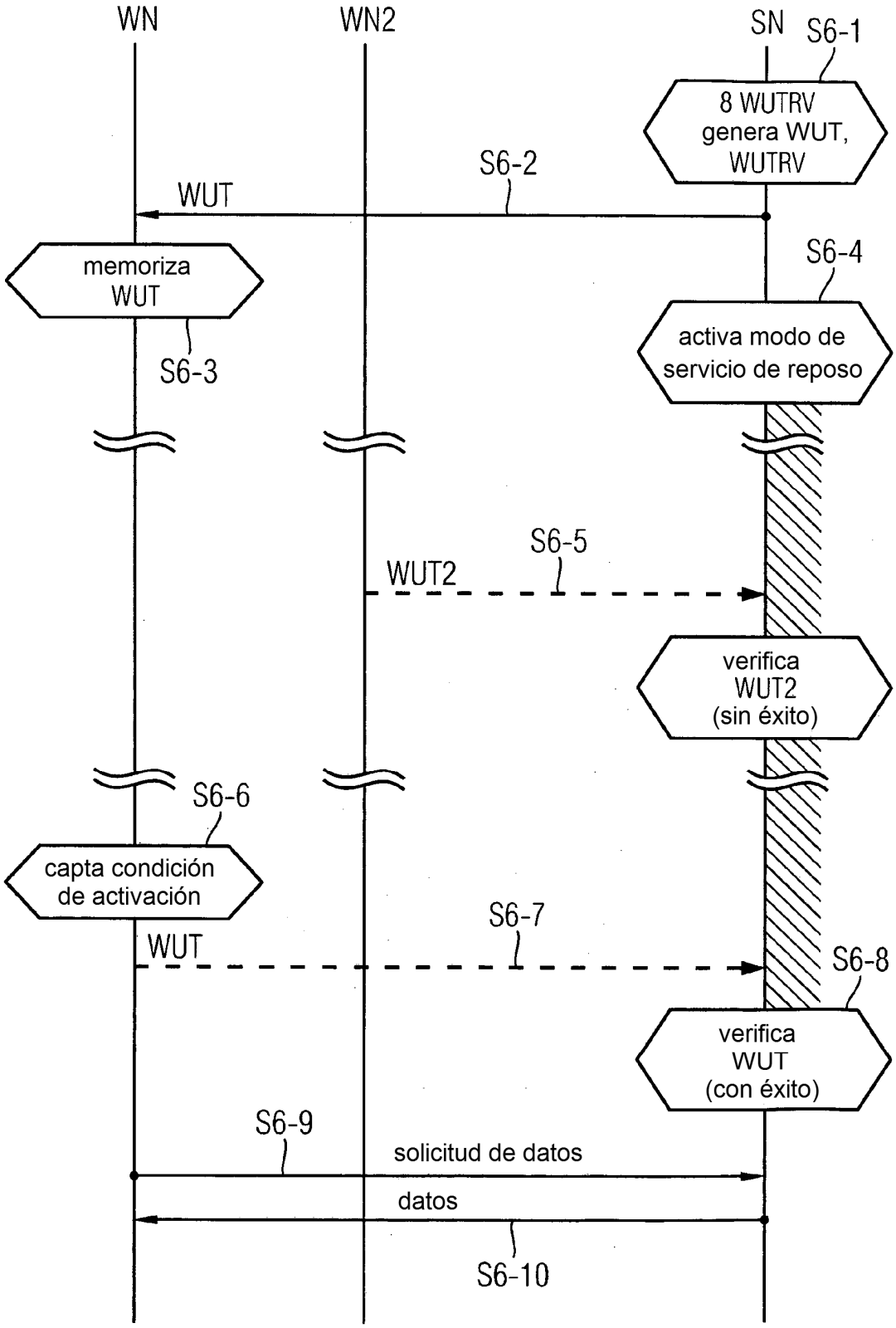

WN
WN2
SN
S6-1
8 WUTRV
genera WUT,
WUTRV
S6-2
WUT
S6-4
memoriza
WUT
activa modo de
servicio de reposo
S6-3
S6-5
WUT2
verifica
WUT2
(sin éxito)
S6-6
capta condición
de activación
S6-7
WUT
S6-8
verifica
WUT
(con éxito)
S6-9
solicitud de datos
datos
S6-10

FIG 7

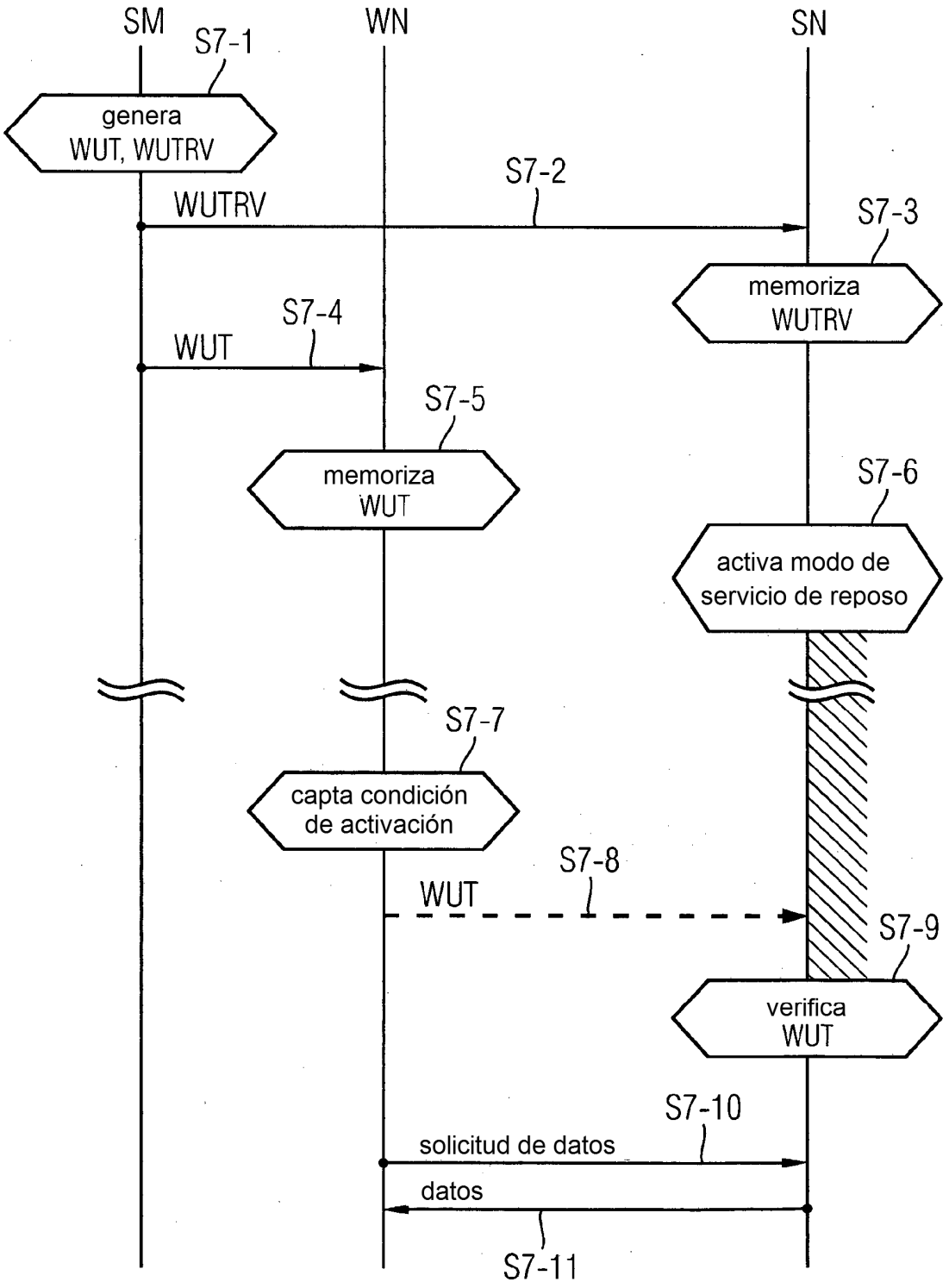

SM
WN
SN
S7-1
genera
WUT, WUTRV
S7-2
WUTRV
S7-3
memoriza
WUTRV
S7-4
WUT
S7-5
memoriza
WUT
S7-6
activa modo de
servicio de reposo
S7-7
capta condición
de activación
S7-8
WUT
S7-9
verifica
WUT
S7-10
solicitud de datos
datos
S7-11

FIG 8

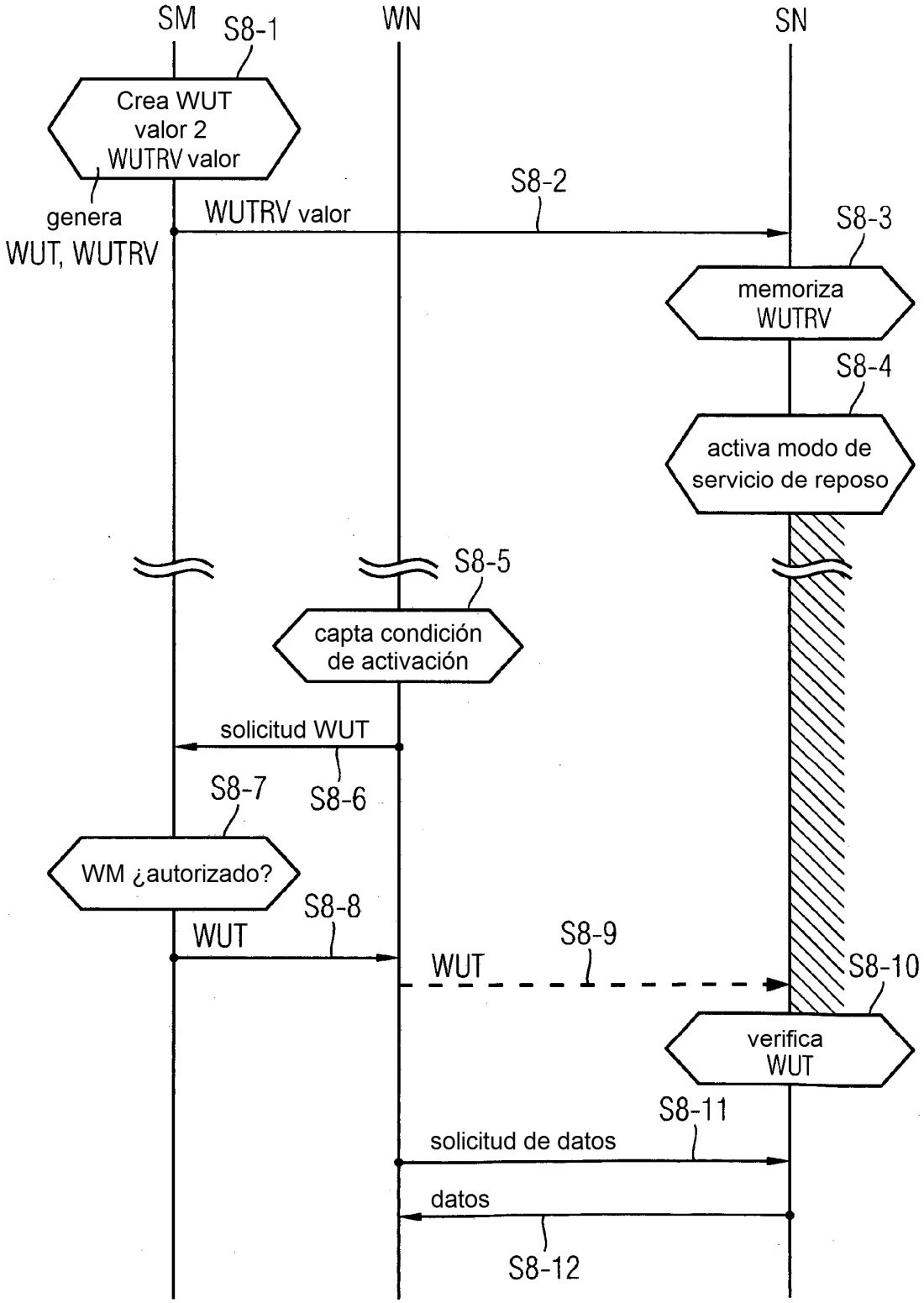

SM
S8-1
WN
SN
Crea WUT
valor 2
WUTRV valor
genera
WUT, WUTRV
WUTRV valor
S8-2
S8-3
memoriza
WUTRV
S8-4
activa modo de
servicio de reposo
S8-5
capta condición
de activación
solicitud WUT
S8-6
S8-7
WM ¿autorizado?
S8-8
WUT
WUT
S8-9
S8-10
verifica
WUT
S8-11
solicitud de datos
datos
S8-12

FIG 9

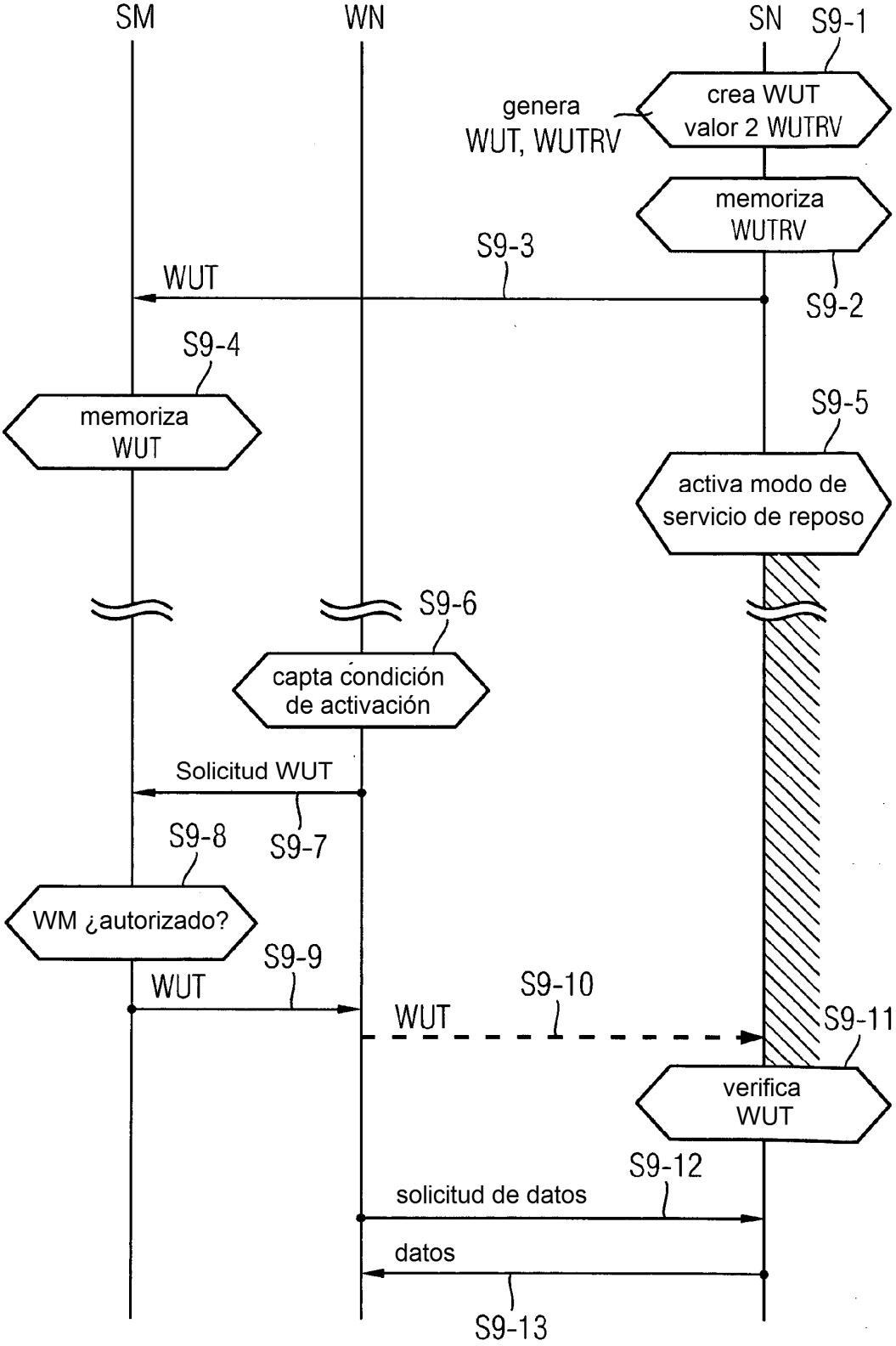

SM
WN
SN
S9-1
crea WUT
valor 2 WUTRV
genera
WUT, WUTRV
memoriza
WUTRV
S9-3
WUT
S9-2
S9-4
memoriza
WUT
S9-5
activa modo de
servicio de reposo
S9-6
capta condición
de activación
Solicitud WUT
S9-7
S9-8
WM ¿autorizado?
S9-9
WUT
S9-10
WUT
S9-11
verifica
WUT
S9-12
solicitud de datos
datos
S9-13

FIG 10

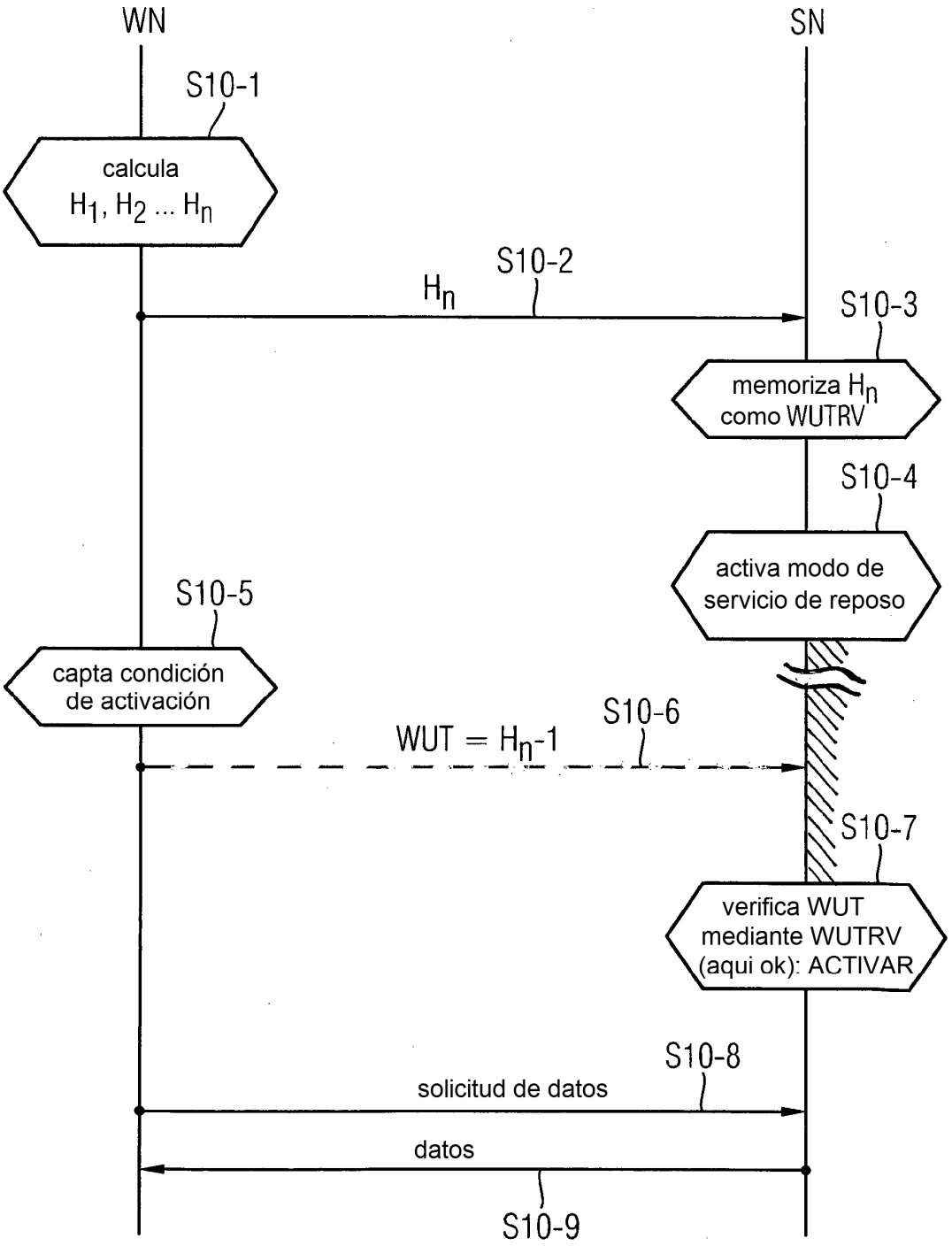
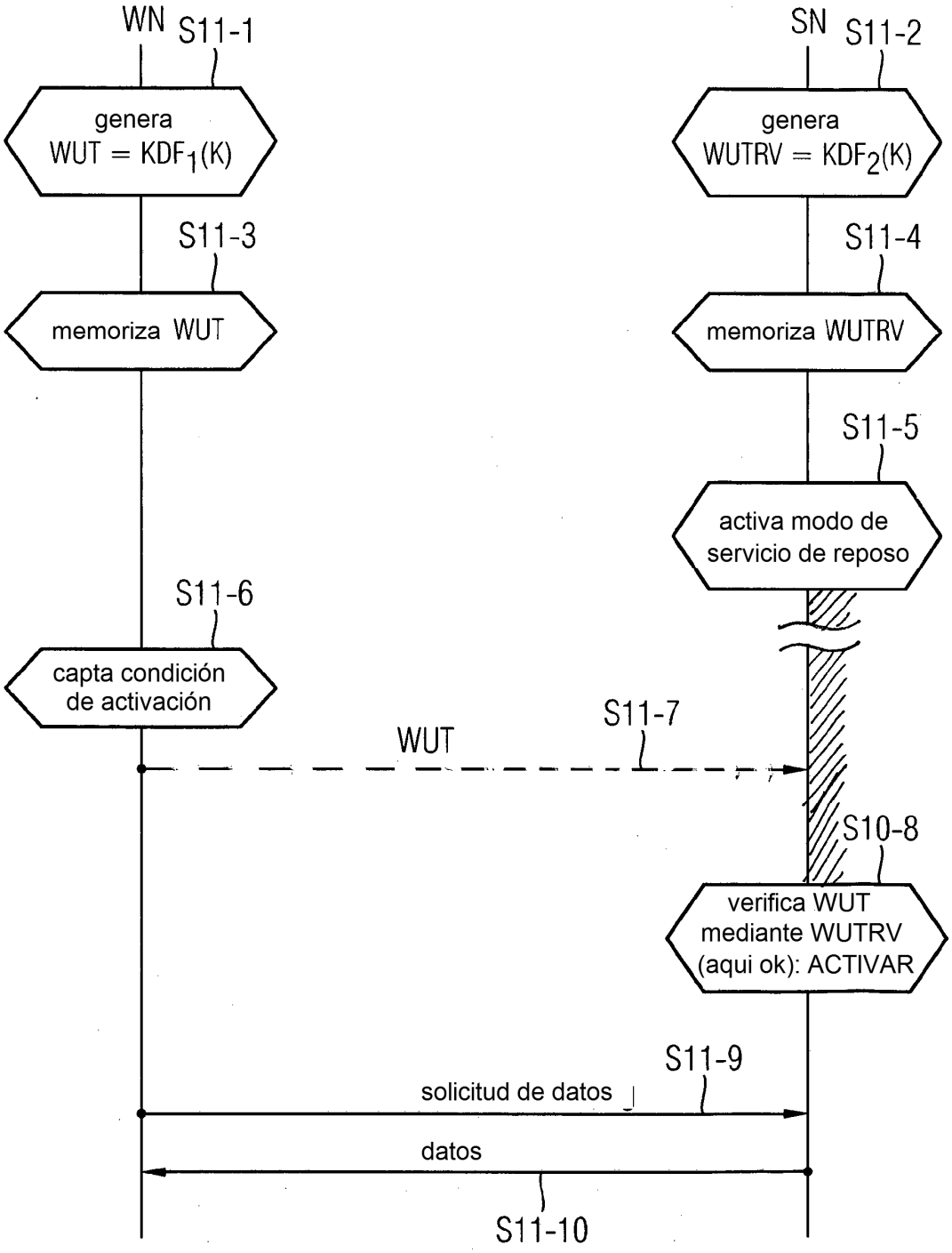

WN
SN
S10-1
calcula
$H_1, H_2 \ldots H_n$
S10-2
H_n
S10-3
memoriza H_n como WUTRV
S10-4
activa modo de servicio de reposo
S10-5
capta condición de activación
S10-6
WUT = H_n-1
S10-7
verifica WUT mediante WUTRV (aqui ok): ACTIVAR
S10-8
solicitud de datos
datos
S10-9

FIG 11


WN
S11-1
genera
WUT = KDF1(K)
S11-3
memoriza WUT
S11-6
capta condición
de activación
SN
S11-2
genera
WUTRV = KDF2(K)
S11-4
memoriza WUTRV
S11-5
activa modo de
servicio de reposo
WUT
S11-7
S10-8
verifica WUT
mediante WUTRV
(aqui ok): ACTIVAR
S11-9
solicitud de datos
datos
S11-10