(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 676 653**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.06.2011 PCT/EP2011/060489**

(87) Fecha y número de publicación internacional: **26.01.2012 WO12010381**

(96) Fecha de presentación y número de la solicitud europea: **22.06.2011 E 11728815 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.05.2018 EP 2572490**

(54) Título: **Procedimiento para el registro de un dispositivo de comunicación inalámbrico en un dispositivo base así como sistema correspondiente**

(30) Prioridad:

22.07.2010 DE 102010031931

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.07.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA EL REGISTRO DE UN DISPOSITIVO DE COMUNICACIÓN INALÁMBRICO EN UN DISPOSITIVO BASE ASÍ COMO SISTEMA CORRESPONDIENTE

DESCRIPCIÓN

La invención se refiere a un procedimiento para el registro de un dispositivo de comunicación inalámbrico así como un sistema correspondiente.

Los aparatos de control, sensores, actuadores se conectan o ponen en red entre sí de forma inalámbrica actualmente cada vez más para garantizar una flexibilidad lo mayor posible. A este respecto, también es más sencillo un mantenimiento de los aparatos o sensores, dado que no se deben abrir canalizaciones de cables, etc., por ejemplo, en el caso de una avería, sino solo directamente el aparato. Para la conexión de los aparatos de control, sensores, etc. se usan habitualmente protocolos abiertos, como IEEE 802.11, WLAN, IEEE 802.15.4, Bluetooth, ZigBee o también Wireless HART. Para evitar a ser posible una manipulación de los sensores o instrucciones de los aparatos de control en la conexión inalámbrica, se encripta criptográficamente la comunicación del aparato de control o sensor por la interfaz puntual correspondiente, por ejemplo, mediante una conexión WLAN mediante TKIP o CCMP o en el caso de 802.15.4 mediante AES-CCM. Para conectar el aparato de control, un sensor o similares con una estación de radio y establecer una conexión encriptada, el aparato de control, el sensor o en general el dispositivo de comunicación inalámbrico se debe configurar de modo que se usa el encriptamiento correspondiente, es decir, establecerse una clave criptográfica. Un dispositivo de este tipo de una clave también se designa como arranque (bootstrapping) o emparejamiento (pairing).

Por el documento US 2006/282885 se conoce que un aparato administrador de un aparato inalámbrico a configurar proporcione de forma inalámbrica un credencial. El aparato inalámbrico se configura por el aparato administrador con el credencial proporcionado por el aparato administrador.

Además se conoce efectuar una comunicación en banda durante una fase débilmente protegida. No obstante, el aparato de comunicación inalámbrico a instalar correspondiente necesita para ello procedimientos de transmisión modificados especiales. Finalmente se conoce efectuar en emparejamiento asegurado por un canal fuera de banda (out-of-band), como por ejemplo interacción humana (es decir, entrada o examen de un PIN, etc.).

A este respecto es desventajoso que los procedimientos mencionados anteriormente requieren una elevada cantidad de trabajo y están configurados de forma complicada, en particular al usarse en el sector industrial, dado que allí se instalan un elevado número de dispositivos de comunicación inalámbricos. A este respecto se requiere simultáneamente que el emparejamiento se realice de forma protegida o asegurada, dado que a este respecto se establecen los parámetros de configuración de seguridad.

Un objetivo de la presente invención es por ello poner a disposición un procedimiento y un sistema para el registro de un dispositivo de comunicación inalámbrico en un dispositivo base, en el que el proceso del emparejamiento para una pluralidad de aparatos inalámbricos a registrar se pueda realizar de forma más sencilla con baja cantidad de trabajo y simultáneamente el proceso de emparejamiento se desarrolle de forma protegida.

Este objetivo se consigue mediante un procedimiento según la reivindicación 1 y un sistema según la reivindicación 7. A este respecto, la ventaja obtenida es que para el registro del dispositivo de comunicación inalámbrico en el aparato base no se necesita una interacción adicional, solo se debe llevar consigo un dispositivo de autentificación correspondiente, por ejemplo, por un montador, etc., a fin de preparar el dispositivo de comunicación inalámbrico para un emparejamiento con el dispositivo base.

Ventajosamente la emisión de una información de autentificación se realiza mediante una potencia de emisión reducida y/o de forma dirigida, de modo que la información de autentificación solo se puede recibir de forma limitada espacialmente. En este caso es ventajoso que con ello se mejora aún más la seguridad del registro del dispositivo de comunicación inalámbrico, dado que la información de autentificación solo se puede recibir en una zona determinada, que está limitada espacialmente debido al alcance limitado y/o la irradiación dirigida. Así a un atacante potencial se le dificulta la escucha o el espiar las informaciones de autentificación transmitidas.

Convenientemente antes de la emisión de la información de autentificación se realiza una supervisión y/o evaluación de señales, en particular señales de comunicación, del dispositivo de comunicación inalámbrico y/o de otros dispositivos de comunicación inalámbricos que se sitúan en un alcance de radio del dispositivo de autentificación. A este respecto, la ventaja obtenida es que con ello se mejora, por un lado, en conjunto la seguridad del registro del dispositivo de comunicación inalámbrico y simultáneamente se puede aumentar la fiabilidad. Si, por ejemplo, se efectúa una supervisión de señales de radio en el rango de frecuencia del dispositivo de comunicación inalámbrico y realiza la verificación de que aquí se envían y/o reciben señales de radio y/o señales de comunicación inusuales por el dispositivo de comunicación inalámbrico, al usuario del dispositivo de autentificación inalámbrico se le mostrará una información correspondiente, de modo que primeramente se realiza la emisión de la información de autentificación luego cuando se ha encontrado el motivo para las señales de radio y/o comunicación inusuales, a fin

de poder excluir una manipulación del dispositivo de comunicación inalámbrico o una escucha de la comunicación del dispositivo de comunicación inalámbrico con el dispositivo de autentificación inalámbrico.

Ventajosamente las señales supervisadas y/o evaluadas del dispositivo de comunicación inalámbrico se codifican en la información de autentificación, evaluándose en particular las señales codificadas, supervisadas y/o evaluadas mediante el dispositivo base. A este respecto, la ventaja de que con ello se aumenta aún más la seguridad, dado que el dispositivo de comunicación inalámbrico dispone de una información de propiedades de radio y/o señales determinadas, de modo que se pueden constatar las manipulaciones en el dispositivo de comunicación inalámbrico. Si la información de las señales supervisadas y/o evaluadas se codifica en la información de autentificación evaluada por el dispositivo base se evita que un dispositivo de comunicación inalámbrico manipulado en sí envíe un resultado de examen falso deseado al dispositivo base y pese a la manipulación se produzca un registro del dispositivo de comunicación inalámbrico en el dispositivo base. De este modo se aumenta aún más la seguridad.

Convenientemente antes de la emisión de la información de autentificación se realiza una verificación de al menos un parámetro de un entorno de radio. Mediante la supervisión al menos de un parámetro del entorno de radio se pueden reconocer de forma sencilla, por ejemplo, otros equipos inalámbricos o señales parásitas en el entorno, de modo que en presencia de señales parásitas u otras aparatos en el entorno se puede prevenir eventualmente una emisión de la información de autentificación, a fin de evitar manipulaciones o una transmisión errónea de la información de autentificación del dispositivo de autentificación inalámbrico hacia el dispositivo de comunicación inalámbrico.

Para garantizar que el dispositivo de autentificación inalámbrico no se retire con finalidades de manipulación, por ejemplo, de un edificio o de un entorno predefinido, es ventajoso que antes de la emisión de la información de autentificación se produzca una localización del dispositivo de autentificación inalámbrico.

Otras características y ventajas de la invención se deducen de la descripción siguiente de un ejemplo de realización mediante las figuras.

A este respecto muestra

Fig. 1 un procedimiento o un sistema para el registro de un dispositivo de comunicación inalámbrico en una primera forma de realización de la presente invención;

Fig. 2a un procedimiento de transmisión según la primera forma de realización de la presente invención;

Fig. 2b un procedimiento de transmisión para un procedimiento según una segunda forma de realización de la presente invención; así como

Fig. 3 un diagrama de transmisión para un procedimiento según una tercera forma de realización de la presente invención.

La fig. 1 muestra un procedimiento o un sistema para el registro de un dispositivo de comunicación inalámbrico en una primera forma de realización de la presente invención.

En la fig. 1 una referencia 1 designa un dispositivo de autentificación inalámbrico 1 que dispone de una interfaz de radio 1a. El dispositivo de autentificación inalámbrico 1 transmite una información de autentificación AI a través de la interfaz de radio 1a hacia un dispositivo de comunicación inalámbrico 2, que se debe registrar en un dispositivo base 4. En el dispositivo base 4 ya están registrados otros dispositivos de comunicación inalámbricos en forma de nodos sensores 3a, 3b, 3c, 3d, que están conectados entre sí de forma inalámbrica para la transmisión de los datos de sensor y eventualmente también directamente con la interfaz de radio 4a del dispositivo base 4. El dispositivo base 4 está conectado de nuevo con una red 5 y les permite a los nodos sensores 3a, 3b, 3c, 3d el acceso a la red 5 después del registro o autentificación exitoso (Network Join) en el dispositivo base 4. Solo un nodo sensor 3a, 3b, 3c, 3d registrado en el dispositivo base 4 se puede inscribir de forma exitosa en el dispositivo base 4. El dispositivo base 4 accede para ello a la información almacenada a través de los nodos sensores registrados 3a, 3b, 3c, 3d. Después de la transmisión de la información de autentificación AI del dispositivo de autentificación inalámbrico 1 al dispositivo de comunicación inalámbrico 2, este envía la información de autentificación obtenida AI según la fig. 1 a través del nodo sensor 3b y 3c, así como a través de la interfaz de radio 4a al dispositivo base 4, que verifica la información de autentificación AI. Para ello se puede examinar p. ej. una suma de comprobación obtenida en la información de autentificación AI (Message Authentication Code (código de autentificación de mensaje, firma digital)). La suma de comprobación se puede calcular mediante el dispositivo de autentificación inalámbrico 1 usando una clave criptográfica almacenada. Si la información de autentificación AI es válida, mediante el dispositivo base 4 se genera una clave de acceso JK (Join Key) y se envía de vuelta a través de los nodos sensores 3a, 3b, 3c, 3d correspondientes finalmente hacia el dispositivo de comunicación inalámbrico 2. El dispositivo de comunicación inalámbrico 2 está registrado ahora en el dispositivo base 4 y tiene ahora acceso a la red 5 del dispositivo base 4.

La fig. 2 muestra un procedimiento de transmisión según la primera forma de realización de la presente invención.

En la fig. 2a se muestra en detalle la transmisión de la información de los aparatos individuales en sucesión temporal. El dispositivo de autentificación inalámbrico 1 envía una información de autentificación AI al dispositivo de comunicación inalámbrico 2 a registrar. El dispositivo de comunicación inalámbrico 2 envía ahora la información de autentificación recibida AI junto con un número de identificación correspondiente del dispositivo de comunicación inalámbrico 2 a registrar a un nodo sensor adyacente 3b, que envía de nuevo eventualmente a través de otros nodos sensores adyacentes 3a, 3c, 3 y la interfaz de radio 4a del dispositivo base 4 esta información de autentificación AI y el número de identificación correspondiente del dispositivo de comunicación inalámbrico 2 a registrar al dispositivo base 4. El dispositivo base 4 verifica ahora en el registro R_1 la información de autentificación obtenida AI y genera una clave de acceso JK en el caso de verificación exitosa e inscribe el número de identificación del dispositivo de comunicación inalámbrico 2 a registrar en una tabla interna del dispositivo base 4, en la que están inscritos igualmente los nodos sensores 3a, 3b, 3c, 3d autorizado al acceso. La clave de acceso generada JK se transmite luego a través de la interfaz 4a, los nodos sensores 3a, 3c, 3d eventualmente y el nodo sensor adyacente 3b del dispositivo de comunicación inalámbrico 2 a este. Por consiguiente está concluido el proceso de registro. En una variante el dispositivo base 4 inscribe durante el registro R_1 adicionalmente la clave de acceso JK en la tabla interna del dispositivo base 4. En otra variante no representada, a través del dispositivo base 4 se usa, en lugar de una tabla interna del dispositivo base 4, una tabla externa del dispositivo base 4, p. ej. una base de datos o un servicio de directorio.

En la fig. 2b el dispositivo de comunicación inalámbrico 2 transmite, a diferencia de la fig. 2a, adicionalmente por parte del dispositivo de comunicación inalámbrico 2 una clave de acceso JK, que está preconfigurada o se genera por sí misma, a través del nudo sensor adyacente 3b eventualmente a través de otros nodos sensores 3a, 3c, 3d y a través de la interfaz de radio 4a del dispositivo base 4, junto con la información de autentificación AI y un número de identificación en el dispositivo base 4. El registro R_2 en el dispositivo base 4 se realiza ahora de la siguiente manera: El dispositivo base 4 examina la información de autentificación obtenida AI y en el caso de una verificación positiva inscribe el número de identificación y la clave de acceso JK en una tabla para nodos sensores autorizados al acceso. Finalmente la estación base 4 transfiere una señal correspondiente de que fue exitoso el registro a través de la interfaz 4a y los nodos sensores 3a, 3b, 3c, 3d al dispositivo de comunicación inalámbrico 2.

La fig. 3 muestra un diagrama de transmisión para un procedimiento según una segunda forma de realización de la presente invención. En la fig. 3 el dispositivo de autentificación inalámbrico 1 realiza una observación B de un procedimiento de prerregistro de un dispositivo de comunicación inalámbrico 2. Éste transfiere su número de identificación y una clave de acceso JK a través del nodo sensor adyacente 3b y eventualmente otros nodos sensores 3a, 3c, 3d a través de la interfaz de radio 4a al dispositivo base 4. Se realiza un almacenamiento R_3 del número de identificación y de la calve de acceso JK a través del dispositivo base 4. El dispositivo base 4 transfiere además una señal de prerregistro, que contiene la información de que fue exitoso el prerregistro, de vuelta al dispositivo de comunicación inalámbrico 2. En este procedimiento de prerregistro se observa (observación B) y analiza la observación B a través del dispositivo de autentificación inalámbrico 1. En función del resultado del análisis se decide luego si se le transfiere una información de autentificación AI al dispositivo de comunicación inalámbrico 2. En el caso de un resultado positivo del análisis A se transfiere una información de autentificación AI al dispositivo de comunicación inalámbrico 2. Éste de nuevo transmite la información de autentificación obtenida y el número de identificación del dispositivo de comunicación inalámbrico 2 a través de los nodos sensores 3b, 3a, 3c, 3d y la interfaz de radio 4a al dispositivo base 4. En el dispositivo base 4 se realiza un registro R_4, en el que se examina la información de autentificación AI y en el caso de un resultado de examen positivo se inscribe el número de identificación del dispositivo de comunicación inalámbrico 2 y de la clave de acceso JK en una tabla de acceso correspondiente según la descripción de las figuras anteriores. Además, el dispositivo base 4 transfiere una información correspondiente de vuelta al dispositivo de comunicación inalámbrico 2 de que ha sido exitoso un registro del dispositivo de comunicación inalámbrico 2 en el dispositivo base 4.

Aunque la presente invención se ha descrito mediante los ejemplos de realización preferidos anteriores, no está limitada a ellos, sino que se puede modificar de múltiples maneras.

Por ejemplo, es posible transmitir la información de autentificación como multidifusión (broadcast). De esta manera todos los dispositivos de comunicación inalámbricos, que se sitúa en el entorno, pueden recibir esta información de autentificación. Además, es posible transmitir la información de autentificación al dispositivo de comunicación inalámbrico determinado como monodifusión, p. ej. después de una autentificación con un certificado de equipo de un nodo sensor o más en general de un dispositivo de comunicación inalámbrico. S este respecto se pueden realizar otras mediciones referidas al nodo de las propiedades de transmisión, p. ej. su intensidad de señal, se puede comparar con un valor predeterminado o se puede verificar mediante la medición de distancia una distancia entre el dispositivo de autentificación inalámbrico y el dispositivo de comunicación inalámbrico. La información de autentificación AI puede comprender, por ejemplo, una contraseña, una secuencia aleatoria alterna temporalmente con un sello de tiempo con una suma de comprobación criptográfica (Message Authentication Code MAC o firma digital). Además, la información de autorización proporcionada por el dispositivo de autentificación inalámbrico se puede componer de varias informaciones parciales. Por ejemplo, es posible que solo se transmita una información parcial por el dispositivo de comunicación inalámbrico al dispositivo base. Por ejemplo, es posible que el dispositivo de autorización inalámbrico proporcione por ejemplo una tupla, que comprende una información de confirmación o

aserción (p. ej. una aserción SAML) y una clave. El dispositivo de comunicación inalámbrico transmite luego la aserción al dispositivo base y verifica el conocimiento de la clave, no obstante, sin transmitirlo al dispositivo base. Esto se puede realizar, por ejemplo, de manera que el dispositivo base transmite un número aleatorio al dispositivo de comunicación inalámbrico. El dispositivo de comunicación inalámbrico realiza entonces un cálculo en el que el número aleatorio y la clave entran como parámetro, por ejemplo, un HMAC-SHA1 (clave, número aleatorio) y transfiere el resultado de vuelta al dispositivo base, que entonces verifica de nuevo si mediante el resultado el dispositivo de comunicación inalámbrico debe obtener el acceso a la red del dispositivo base.

Una comunicación inalámbrica del aparato de comunicación inalámbrico se puede realizar, por ejemplo, mediante WLAN o Bluetooth.

REIVINDICACIONES

1. Procedimiento para el registro de un dispositivo de comunicación inalámbrico (2) en un dispositivo base (4), con las etapas:

(a) emisión de una información de autentificación (AI) mediante un dispositivo de autentificación inalámbrico (1),

(b) recepción de la información de autentificación enviada (AI) por el dispositivo de comunicación inalámbrico (2), en particular mediante comunicación en banda,

(c) transmisión de la información de autorización recibida (AI) junto con un número de identificación del dispositivo de comunicación inalámbrico (2) mediante el dispositivo de comunicación inalámbrico (2) hacia el dispositivo base (4),

(d) verificación de la información de autentificación transmitida (AI) por el dispositivo base (4), y

(e) integración del dispositivo de comunicación inalámbrico (2) en una red (5) en función del resultado de la verificación,

en el que la información de autentificación (AI) se transmite como multidifusión o como monodifusión, y a este respecto se realizan otras mediciones referidas al nodo de las propiedades de transmisión, a fin de comparar una intensidad de señal con un valor predeterminado y/o verificar una medición de distancia entre el dispositivo de autentificación inalámbrico (1) y el dispositivo de comunicación inalámbrico (2).

2. Procedimiento según la reivindicación 1, en el que

la emisión de una información de autentificación (AI) se realiza mediante una potencia de emisión reducida y/o de forma dirigida, de modo que la información de autentificación (AI) solo se puede recibir de forma limitada espacialmente.

3. Procedimiento según una de las reivindicaciones 1 y 2, en el que

antes de la emisión de la información de autentificación (AI) se realiza una supervisión y/o evaluación de señales, en particular señales de comunicación del dispositivo de comunicación inalámbrico (2) y/o de otros dispositivos de comunicación inalámbricos (3a, 3b, 3c, 3d) que se sitúan en un alcance de radio del dispositivo de autentificación (1).

4. Procedimiento según la reivindicación 3, en el que

las señales supervisadas y/o evaluadas del dispositivo de comunicación inalámbrico (2) se codifican en la información de autentificación (AI), en particular en el que la comunicación supervisada codificada se evalúa por el dispositivo base (4).

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que

antes de la emisión de la información de autentificación (AI) se realiza una verificación de al menos un parámetro de un entorno de radio.

6. Procedimiento según una de las reivindicaciones 1 a 5, en el que

antes de la emisión de la información de autentificación (AI) se realiza una localización del dispositivo de autentificación inalámbrico (1).

7. Sistema para el registro de un dispositivo de comunicación inalámbrico (2), en particular apropiado para la realización del procedimiento según una de las reivindicaciones 1 a 6, con:

(a) un dispositivo de autentificación inalámbrico (1), que está diseñado para emitir una información de autentificación (AI) al dispositivo de comunicación inalámbrico (2),

(b) un dispositivo de comunicación inalámbrico (2) para la recepción de la información de autentificación emitida (AI), en particular mediante comunicación en banda, y para el envío de la información de autentificación (AI) junto con un número de identificación del dispositivo de comunicación inalámbrico (2) a un dispositivo base (4) para el registro del dispositivo de comunicación inalámbrico (2),

(c) en el que el dispositivo base (4) integra el dispositivo de comunicación inalámbrico (2) en una red (5) en función de un resultado de una verificación de la información de autentificación (AI),

en el que la información de autentificación (AI) se transmite como multidifusión o como monodifusión, y a este respecto se realizan otras mediciones referidas al nodo de las propiedades de transmisión, a fin de comparar una intensidad de señal con un valor predeterminado y/o verificar una medición de distancia entre el dispositivo de autentificación inalámbrico (1) y el dispositivo de comunicación inalámbrico (2).

8. Sistema según la reivindicación 7, en el que

el dispositivo de autentificación inalámbrico (1) presenta medios de observación (1a) para la observación de un entorno de radio y/o una localización del dispositivo de autentificación inalámbrico (1).

9. Sistema según una de las reivindicaciones 7 u 8, en el que el dispositivo de autentificación inalámbrico (1) presenta medios para la adaptación de una potencia de emisión.

10. Uso de un sistema según una de las reivindicaciones 7 a 9 para el registro de un dispositivo de comunicación inalámbrico (2).

FIG 1

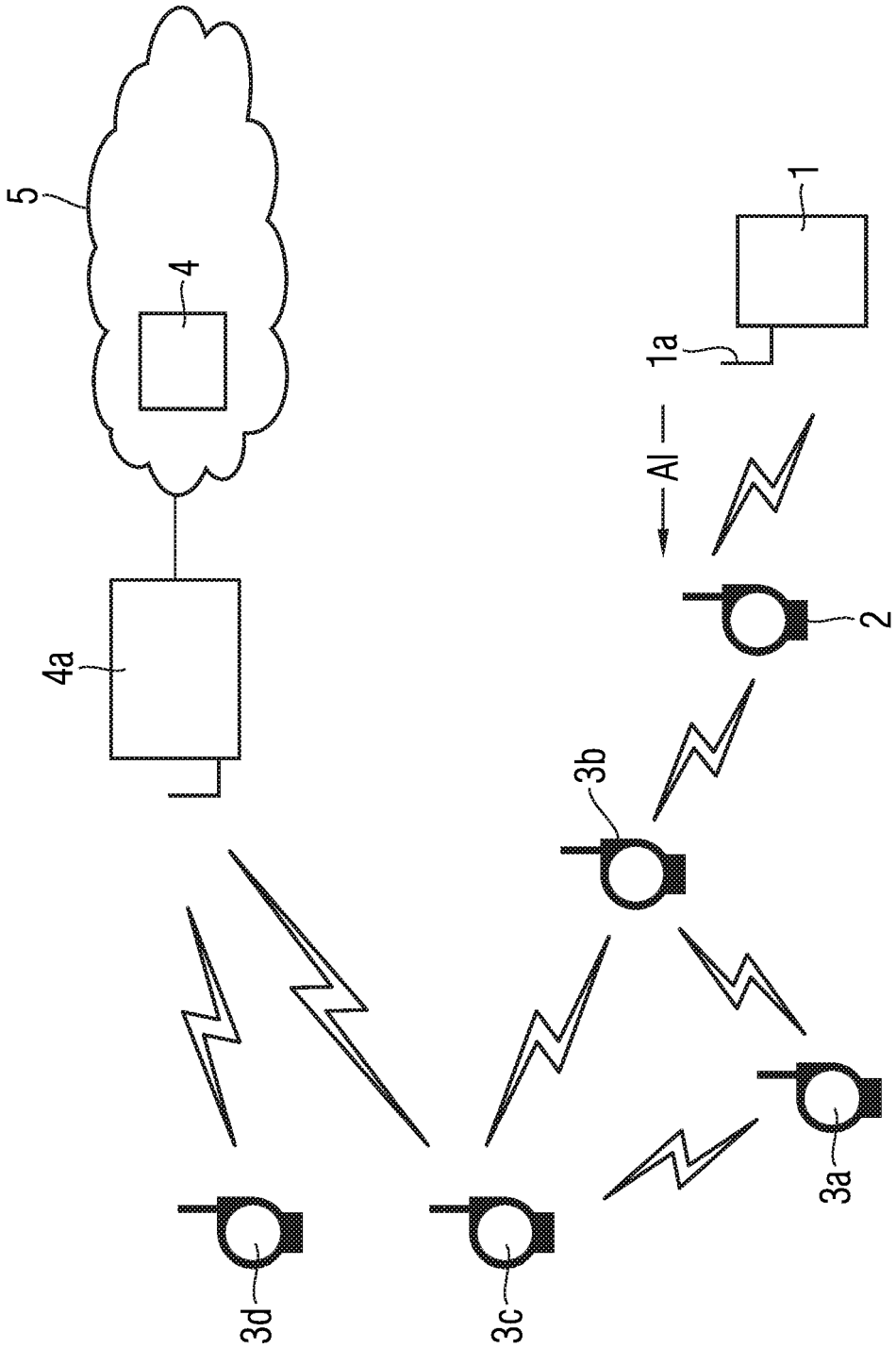


FIG 2A

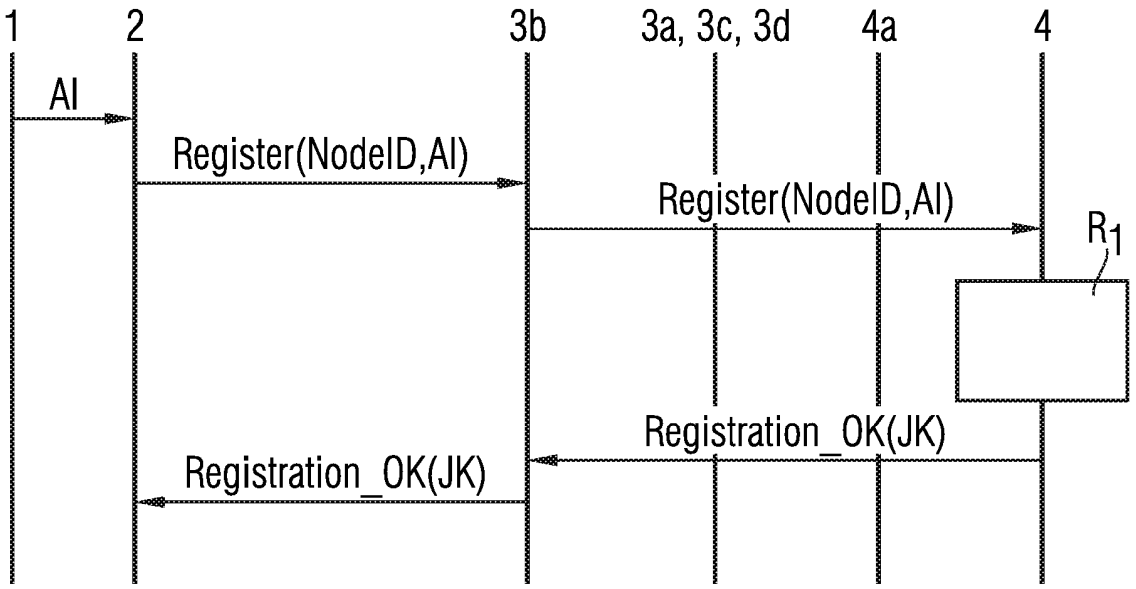

1
2
3b
3a, 3c, 3d
4a
4
AI
Register(NodeID,AI)
Register(NodeID,AI)
R1
Registration_OK(JK)
Registration_OK(JK)

FIG 2B

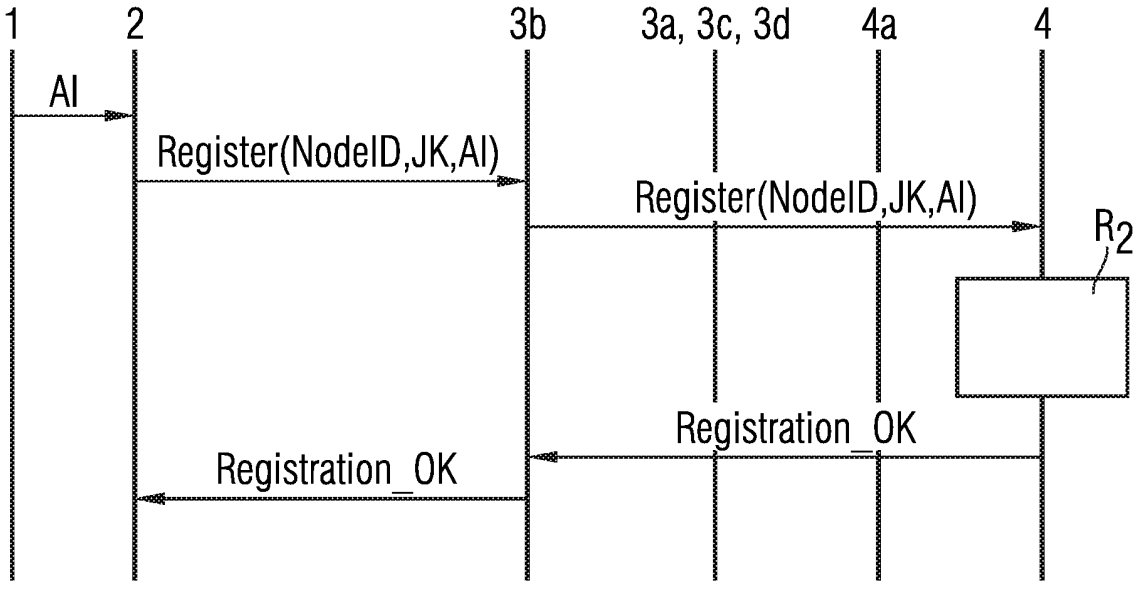
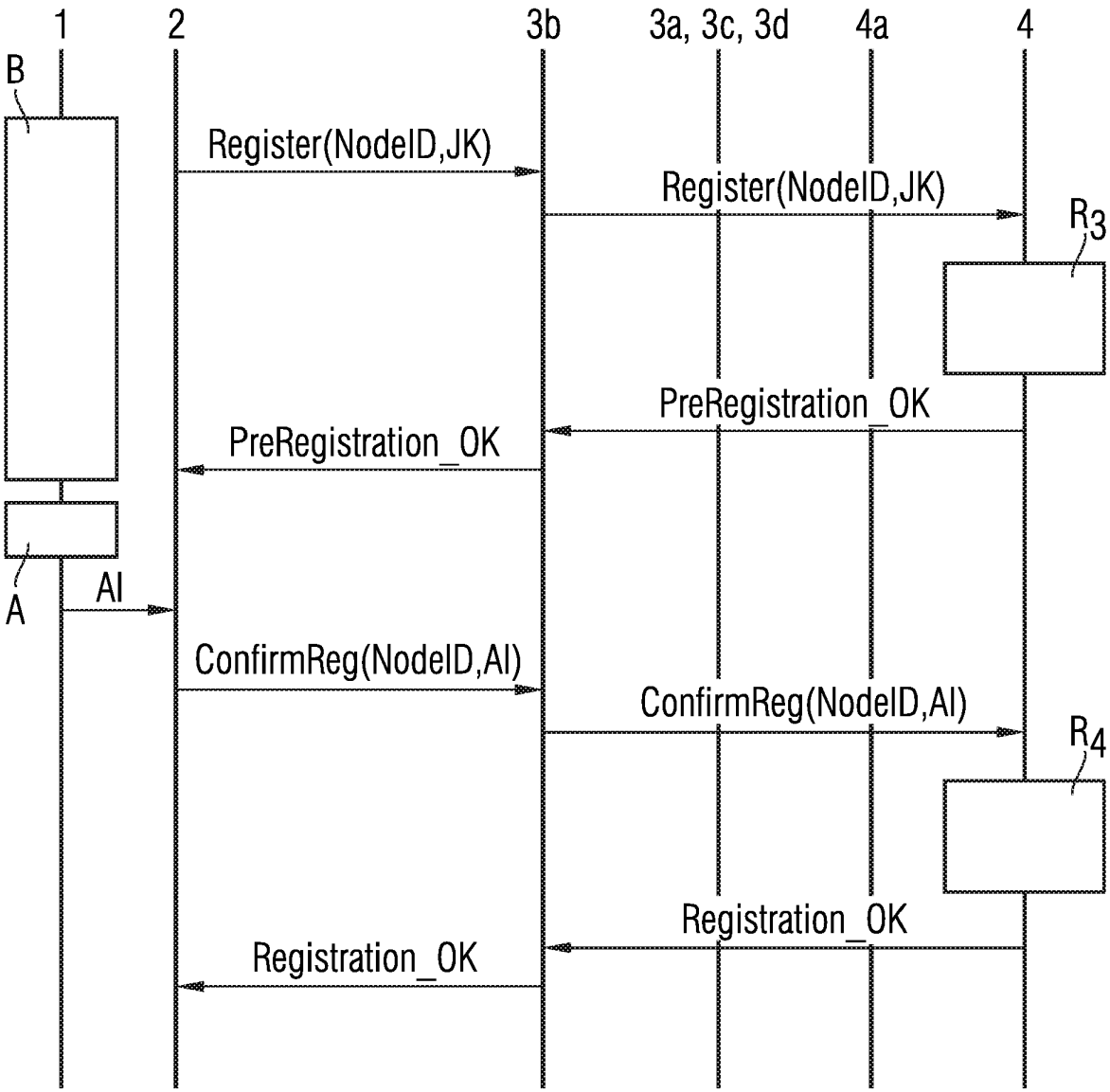

1
2
3b
3a, 3c, 3d
4a
4
AI
Register(NodeID,JK,AI)
Register(NodeID,JK,AI)
R2
Registration_OK
Registration_OK

FIG 3


1
2
3b
3a, 3c, 3d
4a
4
B
Register(NodeID,JK)
Register(NodeID,JK)
R3
PreRegistration_OK
PreRegistration_OK
A
AI
ConfirmReg(NodeID,AI)
ConfirmReg(NodeID,AI)
R4
Registration_OK
Registration_OK