



Patent Application

【Reference Number】 000 2

【Application Classification】 patent application

【Applicant】

【Organization Name】 Samsung Electronics Corporation

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Applicant】

【Organization Name】 Korea Advanced Institute of Science and Technology

【Patent Customer Number】 3 -1 99 8- 0 9 88 66 -1

【Agent】

【Name】 LEE, Keon Joo

【Agent's Code】 9 -1 99 8- 000 33 9 -8

【Registration number of general power of attorney】 200 3-00 14 49 -1

【Title of Invention】 SYSTEM AND METHOD FOR AUTHENTICATING SINK USING MOBILE NETWORK

【English Title of Invention】 S Y S T E M A N D M E T H O D F O R A U T H E N T I C A T I N G S I N K U S I N G M O B I L E N E T W O R K

【Inventor】

【Name】 SHON, Tae Shik

Samsung v. Four Batons
IPR2025-00495
Exhibit 1032





【Name in English】 S H O N , T a e S h i k

【Individual id number】 Secure Information

【Postal code or zip code】 Secure Information

【Address】 Secure Information

【Nationality】 K R

【Inventor】

【Name】 P A R K , Y o n g S u k

【Name in English】 P A R K , Y o n g S u k

【Address】 Secure Information

【Nationality】 U S

【Inventor】

【Name】 H A N , K y u S u k

【Name in English】 H A N , K y u S u k

【Individual id number】 Secure Information

【Postal code or zip code】 Secure Information

【Address】 Secure Information

【Nationality】 K R

【Inventor】

【Name】 K I M , K w a n g J o

【Name in English】 K I M , K w a n g J o

【Individual id number】 Secure Information

【Postal code or zip code】 Secure Information

【Address】 Secure Information



【Nationality】 K R

【Inventor】

【Name】 KIM, Jang Seong

【Name in English】 KIM , Jang Seong

【Individual id number】 Secure Information

【Postal code or zip code】 Secure Information

【Address】 Secure Information

【Nationality】 K R

【Purport】

I submit it to the head of the Korean Intellectual Property Office as above. Darsi in this State (Name or In)

【Official Fee】

【Application Fee】 0 side 38,000 won

【Additional Application Fee】 30 page 0 won

【Priority Fee】 0 case 0 won

【Examination Fee】 0 claim 0 won

【Total】 38,000 won

【Attached Documents】

1. Other attached documents [Delegation of the Korea Advanced Institute of Science and Technology] _1

【Abstract】

【Summary】

The present invention relates to a system and a method for authenticating a sink using a mobile communication network.

To this end, according to the present invention, a mobile terminal transmits a sink authentication request for a sink to a base station, the base station transmits a sink authentication response according to the sink authentication request to the mobile terminal, and the mobile terminal receives the sink authentication response and performs authentication with the sink, thereby reducing time required for authentication.

【Representative Drawing】

Drawing4

【Index Term】

mobile communications network , base station , sync authentication

【Description of the Invention】

【Title of Invention】

SYSTEM AND METHOD FOR SINK AUTHENTICATION USING MOBILE COMMUNICATION NETWORK {S Y S T E M A N D M E T H O D F O R A U T H E N T I C A T I N G S I N K U S I N G M O B I L E N E T W O R K}

【The Detailed Description of the Invention】

【Technical Field】

【0001】 The present invention relates to a system and a method for authenticating a sink, and more particularly, to a system and a method for authenticating a sink by using a mobile communication network.

【Background Technique】

【0002】 In a general sensor network, when a node (n ode) requests a connection with a sink (s ink) connected to the sensor network, the sink transmits information of another connected sink node, and the transmitted information is transmitted to a base station (B as station) through the connected sinks. Upon receiving the node information, the base station performs node authentication and transmits the authentication information back to the synchro. The sink receiving the authentication information of the node performs authentication with the node by determining whether the node is authenticated or not.

【0003】 In such a sensor network, there are various methods for authentication between a node and a sink, and mutual authentication is performed on the sensor network in various methods such as a method of authenticating a device newly participating in the sensor network, generating a link key with the authenticated node, or allowing a base station to be in charge of authentication of the sensor in order to reduce an operation part of the sensor.

【Content of Invention】

【Problem to solve】

【0004】 As described above, in the related art, in order to perform mutual authentication between the node and the sink, information of the node is transmitted to the base station and authentication information is received.

【0005】 However, since the authentication of the node is requested to the base station whenever the node is connected to the sink, in the case of the multi-hop, node information is transferred to the base station through a plurality of sinks, and authentication information needs to be received from the base station.

【0006】 In addition, when authentication is performed through a base station in a sensor network in a multi-hop environment, a large number of sinks need to be performed when authentication is performed, and thus a large number of communication overheads occur, and there is a problem in that a sink detection time and a communication overhead may increase exponentially as the number of hops increases.

【0007】 In addition, when such a node has mobility, there is a growing need to perform authentication between a moving node and a sink using a mobile communication network in order to perform authentication between the moving node and the sink on a multi-hop sensor network.

【0008】 Therefore, the present invention provides a system and a method for performing authentication between a mobile terminal and a sink by using an authentication key generated in advance through authentication between the mobile terminal and a mobile communication network server by using a mobile communication network.

【Solution to the Problem】

【0009】 To this end, the present invention comprises: a mobile terminal



using a mobile communication network. The system for authenticating between sinks comprises: a base station for transmitting a sink authentication response including sink authentication information for a sink to a mobile terminal when there is a sink authentication request for the sink from the mobile terminal; the mobile terminal for transmitting the sink authentication request for the sink to the base station, and authenticating the sink by using the received sink authentication information when the sink authentication response is received from the base station; and the sink for authenticating with the mobile terminal.

【0010】 According to another aspect of the present invention, there is provided a method for authenticating between a mobile terminal and a sink using a mobile communication network in an authentication system including the mobile terminal, the sink, a base station, and a mobile communication network server, the method including: transmitting, by the mobile terminal, a sink authentication request for the sink to the base station; transmitting, by the base station, a sink authentication response according to the sink authentication request to the mobile terminal; and performing, by the mobile terminal, authentication with the sink by receiving the sink authentication response.

【0011】 In addition, the present invention relates to a method for a mobile terminal to authenticate a sink using a mobile communication network, comprising the steps of: transmitting a sink authentication request for the sink to a base station when there is a request for authenticating the sink; and performing an authentication operation with the sink when a sink authentication response for the sink is received from the base station.

【Effect】

【0012】 According to the present invention, when authentication between a mobile terminal and a sink is performed using a mobile communication



network, sink authentication information is received from a base station through the mobile communication network without receiving authentication information from the base station using a sensor network of a multi-hop environment. Therefore, communication and calculation overhead for authentication and key exchange in the sensor network of the multi-hop environment can be reduced, and time required for authentication can be reduced.

【Detailed Description for the Implementation of the Invention】

【0013】 Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. In the following description and the accompanying drawings, a detailed description of known functions and configurations that may unnecessarily obscure the gist of the present invention will be omitted.

【0014】 1 is a diagram illustrating a configuration of a system for mutual increase between a mobile terminal and a sink according to an embodiment of the present invention.

【0015】 The system of the present invention comprises a mobile terminal (100), a plurality of sinks including a first sink (110), a base station (120), a mobile communication network server (130), a mobile communication network (200), and a sensor network (300).

【0016】 When the mobile terminal 100 receives the ID of the first sink 110 together with the HELLO message from the first sink 110, the mobile terminal 100 checks the ID of the first sink 110 to determine whether it is an already authenticated sink.

【0017】 If the first sink 110 is already authenticated, the mobile terminal 100 performs mutual authentication using the shared key generated through the first sink 110. If it is not the pre-authenticated sink, the mobile terminal 100 transmits a sink authentication request message

requesting authentication of the first sink 110 to the base station 120 through the mobile communication network 200.

【0018】 When a sink authentication response message including sink authentication information of the first sink 110 is received from the base station 120, the mobile terminal 100 generates a shared key using the received sink authentication information.

【0019】 Thereafter, the mobile terminal 100 transmits a sync authentication request including shared key generation information for generating a shared key to the first sink 110. The mobile terminal 100 checks the generated shared keys according to a request for checking the shared key from the first sink 110.

【0020】 The first sink 110 periodically broadcasts its own ID together with the H E L L O message for peripheral search. Thereafter, when a sink authentication request including the shared key generation information is received from the mobile terminal 100, the first sink 110 generates a shared key using the received shared key generation information and then requests the mobile terminal 100 to check the shared key.

【0021】 The base station(120) is connected to a plurality of sinks. The authentication information of the connected sinks is stored. When the sync authentication request message is received from the mobile terminal 100, the base station 120 determines whether the mobile terminal 100 that has transmitted the sync authentication request message is an already authenticated mobile terminal, and transmits sync authentication information for authenticating the first sync to the mobile terminal 100 when the mobile terminal 100 is an already authenticated mobile terminal.

【0022】 If the mobile terminal 100 is not authenticated, the base station 120 requests the mobile communication network server 130 to authenticate the mobile terminal 100. At this time, thisThe authentication of the mobile

terminal 100 is the same as the process of authenticating the mobile terminal in general mobile communication.

【0023】 When an authentication response of the mobile terminal 100 is received from the mobile communication network server 130, the base station 120 transmits sink authentication information for authenticating the first sink 110 to the mobile terminal 110.

【0024】 When there is a request for authentication of the mobile terminal 100 from the base station 120, the mobile communication network server 130 transmits a mobile terminal authentication response message including the requested authentication information of the mobile terminal 100 to the base station 120.

【0025】 The mobile communication network 200 is a communication network between the mobile terminal 100, the base station 120, and the mobile communication network server 130. In this case, the mobile terminal 100 generates a shared key between the mobile communication network servers 130 through a G-energy ic B o o ot st ra ping Ar ch it octure (GBA) boot string wrapping process, and performs mutual authentication using the generated shared key. Here, in the GBA bootstrap ping process, a shared key is generated with the mobile communication network server 130 using the seed key Seed key of the user identifier card 40 provided in the mobile terminal 100.

【0026】 The sensor network 300 is a communication network among the mobile terminal 100, the base station 120, and the plurality of sinks.

【0027】 2 is a diagram illustrating a configuration diagram of a mobile terminal according to an embodiment of the present invention.

【0028】 The mobile terminal 100 according to an embodiment of the present invention includes a control unit 10, a sensor 20, a communication module 30, and a user identification card 40.

【0029】 The control unit 10 determines whether the first sink 110 is an already authenticated sink using the ID information of the first sink 110 together with the H E L L O message received from the first sink 110. As a result of the determination, the first sink 110 performs mutual authentication with the first sink 110 using the shared key already generated through the already authenticated sink ramen sensor 20.

【0030】 If the first sink 110 is not authenticated, the sink ramen controller 10 requests the base station 120 to authenticate the first sink 110 through the communication module 30.

【0031】 When a sink authentication response including sink authentication information of the first sink 110 is received from the base station 120 through the communication module 30, the control unit 10 generates a shared key using the received sink authentication information. In this case, the controller 10 stores the generated shared key in the memory of the mobile terminal 100.

【0032】 Thereafter, the control unit 10 transmits a sink authentication request including the shared key generation information to the first sink 110 through the sensor 20.

【0033】 When a response to the sync authentication request is received from the first sink 110, the control unit 10 transmits a request for checking the generated shared key to the first sink 110 through the sensor 20.

【0034】 The sensor 20 receives the ID information of the first sink 110 together with the H E L L O message from the first sink 110 and transmits the received ID information to the control unit 10, and transmits the shared key generation information for generating the shared key to the first sink 110.

【0035】 The communication module 30 receives ID information of the first sink 110 together with the H E L L O message received from the first sink 110 and transmits a sink authentication request message requesting

authentication of the first sink 110 to the base station 120. Moreover, the communications module(30) is the baseA sink authentication response message including sink authentication information of the first sink 110 is received from the tessian 120.

【0036】 The user identifier card 40 stores the shared key generated through the G BA authentication process between the mobile terminal 100 and the mobile communication network server 130. At this time, the user identifier card 40 performs GBA authentication with the mobile communication network server 130 using its own seed key to generate a shared key, and stores the generated shared key in the memory of the mobile terminal 100.

【0037】 As described above, in the present invention, authentication between the mobile terminal and the sink is performed using the sink authentication information received from the base station through the mobile communication network, thereby reducing time required for initial authentication between the mobile terminal and the sink.

【0038】 3 is a flowchart illustrating a process of performing authentication with a sink in a mobile terminal according to an embodiment of the present invention.

【0039】 In step 300, the control unit 100 finds the first sink 110 by receiving the ID of the first sink 110 together with the HEL L O message from the first sink 110 through the sensor 20.

【0040】 In step 302, the control unit 100 determines whether the found first sink 110 is an already authenticated sink, proceeds to step 3 and 12 if the found first sink 110 is an already authenticated sink, and otherwise proceeds to step 30 and 4 to request authentication of the first sink 110 from the base station 120. In this case, the base station 120 transmits the authentication request for the mobile terminal 100 having made the authentication request to the mobile communication network server 130, and when the mobile

terminal 100 is authenticated through the mobile communication network server 130, the base station 120 transmits a sink authentication response including sink authentication information for the first sink 110 to the mobile terminal 100.

【0041】 When the sink authentication response is received from the base station 120 through the communication module 30 in step 306, the control unit 100 generates a shared key using the sink authentication information received as the sink authentication response.

【0042】 3 In step 10, the control unit 100 transmits shared key generation information including the generated shared key to the first sink 110 through the sensor 20.

【0043】 30 2 steps and 3 10 steps and 3 12 steps The control unit 100 performs an authentication operation with the first sink 110, checks the generated shared key, and ends the authentication process.

【0044】 Through this authentication process, initial authentication between the mobile terminal and the sink can be performed more quickly.

【0045】 4 is a flowchart illustrating a process of performing authentication between a mobile terminal and a sink in an authentication system according to an embodiment of the present invention

【0046】 In the embodiment of the present invention, it is assumed that the mobile terminal 100 has not yet been authenticated with the mobile communication network server 130 and the first sink 110 has not yet been authenticated with the mobile terminal 100.

【0047】 In step 400, the first sink 110 periodically broadcasts related information together with the H E L L O message.

【0048】 Specifically, the first sink 110 generates a time stamp TS and a random number R AND indicating the H E L L O message generation time together with the H E L L O message, and authentication information $u[0]=enc$

{CK_S1, R AND|TS} indicating that the generated H E L L O message, TS, and R AND are the first sink S1It is created. In this case, $u[0]$ is information obtained by encrypting TS and R AN D with an encryption key C K_S1 shared between the base station 120 and the first sink 110. In addition, the first sink 110 generates the integrity information of the generated $u[0]$, $v[0]=MAC\{I K_S1, S1||u[0]\}$. Here, IK_S1 means an integrity check key shared between the base station 120 and the first sink 110.

【0049】 Thereafter, the first sink 110 broadcasts S1, $u[0]$, and $v[0]$, which are IDs of the first sink, together with the generated H E L L O message.

【0050】 The mobile terminal 100 receiving the related information together with the H E L L O message checks the received information on the ID of the first sink 110 to check whether it is a sink that has already been authenticated with the mobile terminal 100. If it is an already authenticated sink, mutual authentication is performed using the shared key generated during authentication.

【0051】 If the first sink 110 is not authenticated, the mobile terminal 100 generates a sink authentication request message for requesting authentication of the first sink to the base station 120 in step 40. Then, the mobile terminal 100 generates authentication information $u[1]=enc\{CK_MD, S1||u[0]||v[0]\}$ obtained by encrypting S1, $u[0]$, and $v[0]$ with an encryption key CK_MD shared between the base station 120 and the mobile terminal 100, and generates integrity information $v[1]=MAC\{I K_MD, MD|BS||S1||APP_REQ||u[1]\}$ for integrity checking of $u[1]$. Here, IK_MD denotes an integrity check key shared between the base station 120 and the mobile terminal 100. In addition, the encryption key C K_MD and the integrity key I K_MD are generated through the G BA boot st ra ping operation of the mobile communication network server 130 and the mobile terminal 100 performed before step 401.It is done. In this case, the GBA bootstrapping operation refers to an operation

of generating a shared key between the mobile terminal 100 and the mobile communication network server 130 using the user identification card 40 and then performing authentication therebetween.

【0052】 Thereafter, the mobile terminal 100 transmits the ID MD, $u [1]$, and $v [1]$ of the mobile terminal 100 to the base station 120 together with the generated sync authentication request message to request sync authentication.

【0053】 Upon receiving the request, the base station 120 checks the received ID of the mobile terminal 100 to determine whether the mobile terminal 100 requesting sync authentication is an already authenticated mobile terminal. As a result of the determination, when the mobile terminal is not authenticated, the base station 120 requests authentication of the mobile terminal 100 from the mobile communication network server 130 in step 402.

【0054】 In step 403, the mobile communication network server 130 transmits a mobile terminal authentication response message including an encryption key and an integrity key of the mobile terminal 100 shared in advance to the base station 120 through a GBA operation such as 3G PP TS 33.2 20.

【0055】 In step 404, the base station 120 generates a sink authentication response message including sink authentication information for authenticating the first sink 110 using the received encryption key and integrity key of the mobile terminal 100, and then transmits the generated sink authentication response message to the mobile terminal 100.

【0056】 Specifically, the base station 120 is an encryption key $C K_{S1}$ shared with the first sink together with the sink authentication response message, an arbitrary random number $R A N D$, a time stamp $T S$, and the like. $u [2] = e n c$ in which $h (R A N D || C K_{M D})$ and $h (R A N D || I K_{M D})$ are encrypted $\{C K_{S1}, R A N D | T S | h (R A N D || C K_{M D}) | h (R A N D || I K_{M D})\}$ is generated. Here, $h (R A N D || C K_{M D})$ is a value obtained by applying a hash function to

the encryption key and the random number of the mobile terminal 100, and $h(RAND||IK_{MD})$ is a value obtained by applying a hash function to the integrity key and the random number of the mobile terminal 100. These $h(RAND||CK_{MD})$, $h(RAND||IK_{MD})$ are used to generate a shared key between the mobile terminal 100 and the first sink 110.

【0057】 In addition, the base station 120 generates integrity information $v[2]=MAC\{IK_{S1}, BS|S1|MD|RAND|u[2]\}$ for integrity checking of $u[2]$.

【0058】 Thereafter, the base station 120 generates $u[3] = enc\{CK_{MD}, RAND||TS||h(RAND||CK_{S1})|h(RAND||IK_{S1})|u[2]|v[2]\}$ in which an arbitrary random number, a time stamp (TS) indicating the time at which the authentication response message was generated, $h(RAND||CK_{S1})$, $h(RAND||IK_{S1})$, $u[2]$ and $v[2]$ are encrypted with CK_{MD} . In addition, the base station 120 generates integrity information $v[3]=MAC\{IK_{MD}, BS|MD|S1|APP_RES|u[3]\}$ for integrity checking of $u[3]$. In this case, APP_RES means an authentication response message.

【0059】 The base station 120 transmits the ID_{MD} , $u[3]$, and $v[3]$ of the mobile terminal 100 to the mobile terminal 100 together with the generated sync authentication response message.

【0060】 In step 405, the mobile terminal 100 generates a shared key for authentication with the first sink 120 according to the sink authentication response.

【0061】 Specifically, the mobile terminal 100 checks the integrity of $u[3]$ by checking the received $v[3]$, releases the encryption of the received $u[3]$ by using its own encryption key, and then makes a random egg. The numbers $RAND$, $h(RAND||CK_{S1})$, $h(RAND||IK_{S1})$, $u[2]$, $v[2]$ are detected.

【0062】 Thereafter, the mobile terminal 100 generates a sync authentication request message, and generates a shared key $CK_{S1_MD}=KDF(h(RAND||CK_{S1}), h(RAND||CK_{S1}))$ and an integrity key $IK_{S1_MD}=KDF(h(RAND$

$D||CK_MD)$) for authentication with the first sink 110 using the detected R_AND , $h(R_AND||CK_S1)$, $h(R_AND||CK_S1)$, and its own encryption key. In addition, the mobile terminal 100 generates integrity information $v[4]=MAC\{IK_S1_MD, AUTHREQ | MD | S1 | R_AND | u[2] | v[2]\}$. In this case, $v[4]$ is information for confirming that $u[2]$ and $v[2]$ are information received from the mobile terminal 100.

【0063】 Referring to (a) of FIG. 5, the mobile terminal 100 applies a hash function to an arbitrary random number R_AND and its own encryption key CK_MD , and again applies the hash function to the applied value and $h(R_AND||CK_S1)$ to generate the shared key CK_S1_MD . In addition, the mobile terminal 100 generates the integrity key IK_S1_MD by using $h(R_AND||IK_S1)$ in the same manner as described above.

【0064】 In step 406, the mobile terminal 100 transmits its own ID MD , $u[2]$, $v[2]$, and $v[4]$ to the first sink 110 together with the generated sink authentication request message ($AUTHREQ$).

【0065】 In step 407, the first sink 110 generates a shared key according to the received sink authentication request message.

【0066】 Specifically, the first sink 110 checks the received $v[2]$ to perform the integrity check of $u[2]$, and decodes $u[2]$ to calculate an arbitrary random number R_AND , a time stamp TS , $h(R_AND||CK_MD)$, and $h(R_AND||IK_MD)$ for generating a shared key. Thereafter, the first sink 110 is calculatedAfter generating the shared key CK_S1_MD and the integrity key IK_S1_MD for authentication with the mobile terminal 100 by using R_AND , $h(R_AND||CK_MD)$, and $h(R_AND||IK_MD)$, $v[4]$ is checked to confirm that the information transmitted together with the currently transmitted sync authentication request message is received from the mobile terminal. In this case, the validity period of the generated shared key CK_S1_MD and the integrity key IK_S1_MD is the time stamp TS .

【0067】 An operation of generating the shared key in the first sink 110 will be described with reference to (b) of FIG. 5. The first sink 110 applies a hash function to an arbitrary random number R AND and its own encryption key C K_S1 and applies a hash function to the applied value and $h(R \text{ AND} || \text{CK_MD})$ again to generate the shared key C K_S1_MD. In addition, the first sink 110 generates the integrity key I K_S 1_MD by using $h(R \text{ AN D} || \text{I K_MD})$ in the same manner as described above.

【0068】 In step 408, the first sink 110 transmits a sink authentication response to the sink authentication request to the mobile terminal 100.

【0069】 Specifically, the first sink 110 generates a sink authentication response message, receives information for authentication from the mobile terminal 100 within a period in which a random number is generated, and generates information $v [5] = \text{M AC} \{ \text{I K_S 1_MD}, \text{A UT H RE S} || \text{S 1} | \text{MD} | \text{R AN D} \}$ for notifying that a shared key is generated using the received information. Thereafter, the first sink 110 transmits its own ID S1, the ID MD of the mobile terminal, and $v[5]$ to the mobile terminal 100 together with the sink authentication response message A UT H RE S.

【0070】 In step 409, the mobile terminal 100 transmits an authentication confirmation message to the first sink 110.

【0071】 Specifically, the mobile terminal 100 checks the received $v [5]$, and checks that the first sink 110 has generated the shared key using the authentication information sent by the mobile terminal 100. Thereafter, the mobile terminal 100 generates an authentication confirmation message A UT H CO N, checks the validity of the random number, and generates information $v [6] = \text{M AC} \{ \text{I K_S 1_MD}, \text{A UT H CO N} || \text{MD} | \text{R AN D} + 1 \}$ for notifying that the authentication operation has been performed within the period in which the random number is generated.

【0072】 The mobile terminal 100 transmits its own ID MD, ID S1 of the

first sink 110, and v [6] to the first sink 110 together with the generated authentication confirmation message.

【0073】 4 In step 10, the first sink 110 checks the received information and completes authentication. Specifically, the first sink 110 checks the received v [6] and completes the authentication process with the mobile terminal 100 if it is valid.

【0074】 Steps 40 8-4 10 as described above are processes that can be selectively performed.

【0075】 Referring to FIG. 6, a process of generating a shared key between the mobile terminal 100 and the first sink 110 will be described. The mobile terminal 100 performs a GBA authentication process with the mobile communication network server 130 using the seed key of the user identifier card 40, and stores the encryption key CK_{MD} and the integrity key IK_{MD} generated through the GBA authentication process in advance. The reason why the encryption key and the integrity key generated through the GBA authentication process are stored in advance is to minimize the role of the user identifier card 40, to safely protect the seed key stored in the user identifier card 40 even when the shared key is leaked, and to facilitate the connection between the mobile communication network and the sensor network compared to the existing network connection method.

【0076】 Thereafter, the mobile terminal 100 authenticates its own encryption key CK_{MD} when authenticating the first sink 110, and performing authentication with the base station (120) using the integrity key IK_{MD} , and generating the shared key CK_{S1_MD} and the integrity key IK_{S1_MD} using the sync authentication information received through the base station (120).

【0077】 The first sink 110 also generates the CK_{S1_MD} and the integrity key IK_{S1_MD} using the sink authentication information received from the mobile terminal 100 together with the encryption key CK_{MD} and the



integrity key I K_MD thereof.

【0078】 When the first sink 110 is to be re-authenticated, if the mobile terminal 100 and the first sink 110 are connected to each other, the mobile terminal 100 confirms the authentication with the first sink 110 and then transmits the authentication information on the adjacent sink to the first sink 110 to perform the re-authentication operation. In addition, when the mutual authentication between the mobile terminal 100 and the first sink 110 is not performed, the mobile terminal 100 performs the above-described authentication operation to perform the authentication with the first sink 110.

【0079】 As described above, according to the present invention, authentication between the base station and the mobile terminal is performed through the mobile communication network when mutual authentication between the mobile terminal and the sink is performed, and authentication with the sink is performed using the sink authentication information received from the base station, thereby reducing communication and calculation overhead for authentication and key exchange in a sensor network in a multi-hop environment, and reducing time required for authentication.

【Claims】

【Claim 1】

as to the system for authentication between the mobile terminal and sink by using the mobile radio communications network

a base station which transmits a sink authentication response including sink authentication information for the sink to the mobile terminal when there is a sink authentication request for the sink from the mobile terminal

a mobile terminal transmitting a sink authentication request for the sink to the base station, and authenticating the sink by using the received sink authentication information when a sink authentication response is received from the base station

an authentication system including the sink for authenticating the mobile terminal.

【Claim 2】

The method of claim 1,

An authentication system further comprising: a mobile communication network server configured to transmit an authentication response in response to an authentication request for the mobile terminal.

【Claim 3】

The mobile terminal of claim 1, wherein the mobile terminal comprises:

a step of determining whether the sink is an already authenticated sink if there is a request for authenticating the sink, and a step of determining whether the sink is an unauthenticated sink if the sink is checkedAn authentication system characterized in that it transmits a sync authentication request message for the sync to this shunt.

【Claim 4】

The base station of claim 3

When the sync authentication request message is received from the mobile terminal, it is determined whether the mobile terminal is an already authenticated mobile terminal, and when the mobile terminal is an unauthenticated mobile terminal, a mobile terminal authentication request message for requesting authentication of the mobile terminal is transmitted to the mobile communication network server.

【Claim 5】

The mobile communication network server of claim 4,

When a mobile terminal authentication request message is received from the base station, a mobile terminal authentication response message including mobile terminal authentication information generated in advance through authentication with the mobile terminal is generated and transmitted to the base station.

【Claim 6】

The base station of claim 5

When the mobile terminal authentication response message is received from the mobile communication network server, the mobile terminal is authenticated using the mobile terminal authentication information, and a sink authentication response message including sink authentication information for the sink is generated and transmitted to the mobile terminal.

【Claim 7】

The mobile terminal of claim 6, wherein the mobile terminal comprises:

When the sink authentication response message is received from the mobile communication network server, a shared key for authentication between the sinks is generated using the sink authentication information, and then the sink and the authentication are performed using the generated shared key.

【Claim 8】

as to the method for authentication between the mobile terminal and sink
by using the mobile radio communications network in the authentication
system including the mobile terminal , sink , base station , mobile radio
communications network server

A process of transferring to the mobile terminal is the base station the sink
authentication request about sink

A process of transferring to the base station this mobile terminal the sink
authentication response according to the sink authentication request
and a step in which the mobile terminal performs authentication with the sink
by receiving the sink authentication response.

【Claim 9】

The method of claim 8, wherein the mobile terminal transmits a sync
authentication request for the sync to the base station
a sink in which the sink is already authenticated if there is a request for
authenticating the sink a process of deciding whether or not
and a step of transmitting a sink authentication request message for the
sink to the base station when the sink is not authenticated as a result of the
determination.

【Claim 10】

The method of claim 9, wherein the base station transmits a sync
authentication response according to the sync authentication request to the
mobile terminal
a step of determining whether the mobile terminal is an already authenticated
mobile terminal when a sync authentication request message is received from
the mobile terminal
a step of transmitting a mobile terminal authentication request message

requesting authentication of the mobile terminal to the mobile communication network server when the mobile terminal is not authenticated as a result of the determination

a step of receiving a mobile terminal authentication response message including mobile terminal authentication information generated in advance through authentication with the mobile terminal from the mobile communication network server

A process of authenticating the mobile terminal through the received mobile terminal authentication information as described above and a step of generating a sink authentication response message including sink authentication information for the sink and transmitting the generated sink authentication response message to the mobile terminal.

【Claim 11】

The method of claim 10, wherein the mobile terminal performs authentication with the sink by receiving the sink authentication response a step of generating a shared key for authentication between the sinks using the sink authentication information when the sink authentication response message is received from the mobile communication network server and performing authentication with the sink by using the generated shared key.

【Claim 12】

, and the method for the mobile terminal using the mobile radio communications network and performing authentication with sink a step of transmitting a sink authentication request for the sink to a base station if there is a request for authenticating the sink and performing an authentication operation with the sink when a sink authentication response with respect to the sink is received from the base



station.

【Claim 13】

The method of claim 12, wherein the transmitting of the sync authentication request for the sink to the base station comprises:

The process of determining whether sink is the already authenticated sink or not according to the request for authenticating sink

and a step of transmitting a sink authentication request message for the sink to the base station when the sink is not authenticated as a result of the determination.

【Claim 14】

The method of claim 13, wherein performing the authentication operation with the sink comprises:

A process of being created the shared key for authentication between sink

it uses the sink authentication information the sink authentication response message is received from the mobile communications network server

and a process of performing authentication with the sink by transferring the shared key generation information using the generated shared key to the sink.



【Description of Drawings】

【0080】 1 is a diagram showing a configuration of a system for mutual increase between a mobile terminal and a sink according to an embodiment of the present invention

【0081】 2 is a diagram showing a configuration of a mobile terminal according to an embodiment of the present invention

【0082】 3 is a flowchart illustrating a process of performing authentication with a sink in a mobile terminal according to an embodiment of the present invention

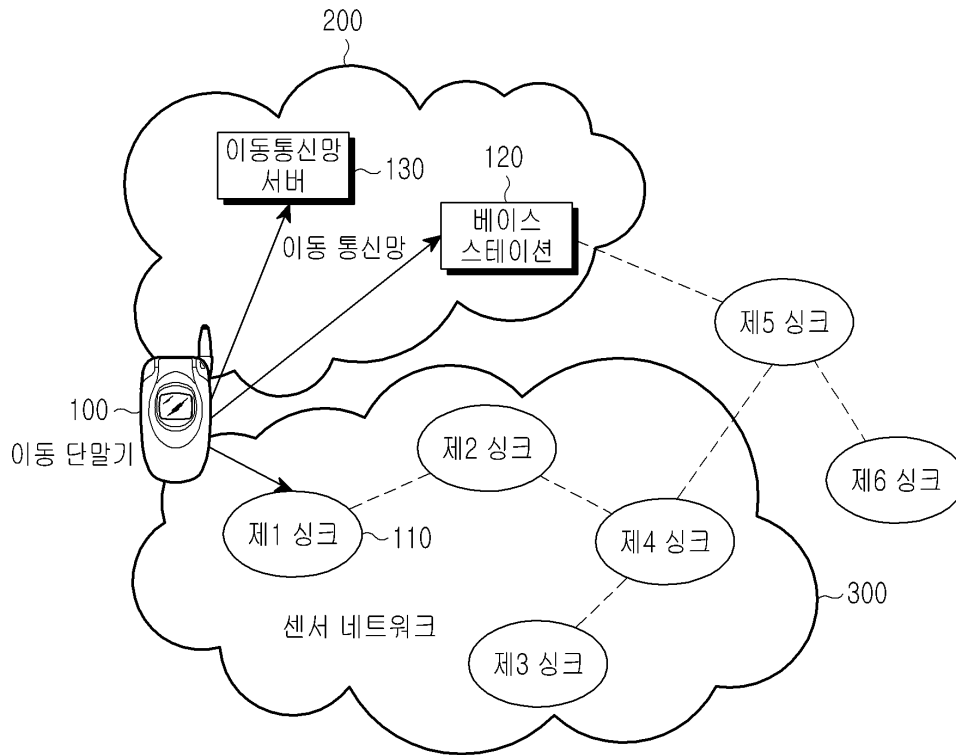
【0083】 4 is a flowchart illustrating a process of performing authentication between a mobile terminal and a sink in an authentication system according to an embodiment of the present invention

【0084】 5 is an exemplary diagram for explaining a shared key generated in each of a mobile terminal and a sink according to an embodiment of the present invention

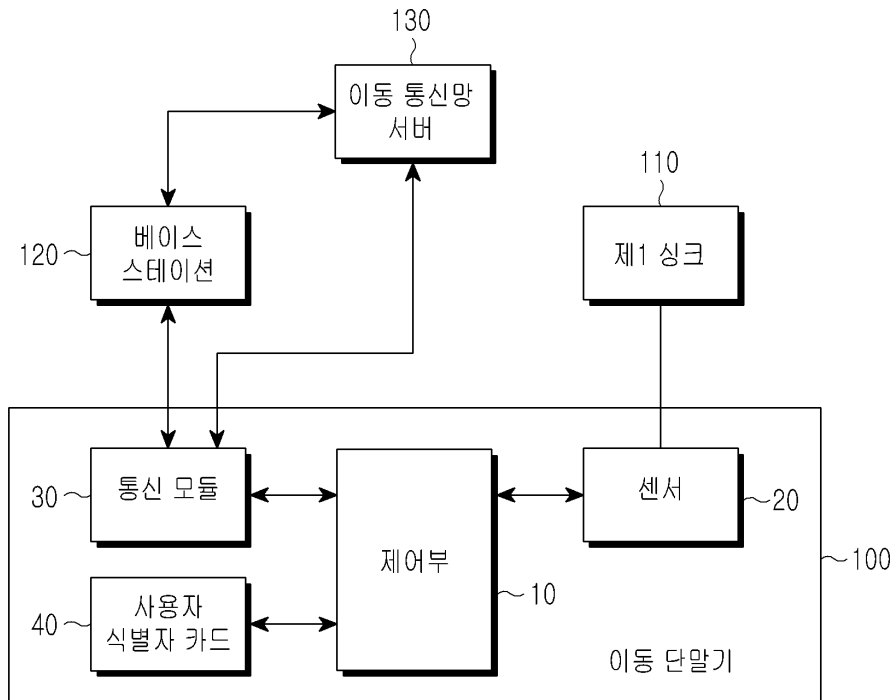
【0085】 6 is an exemplary diagram for explaining keys generated through authentication between a mobile terminal and a sink according to an embodiment of the present invention.

【Drawings】

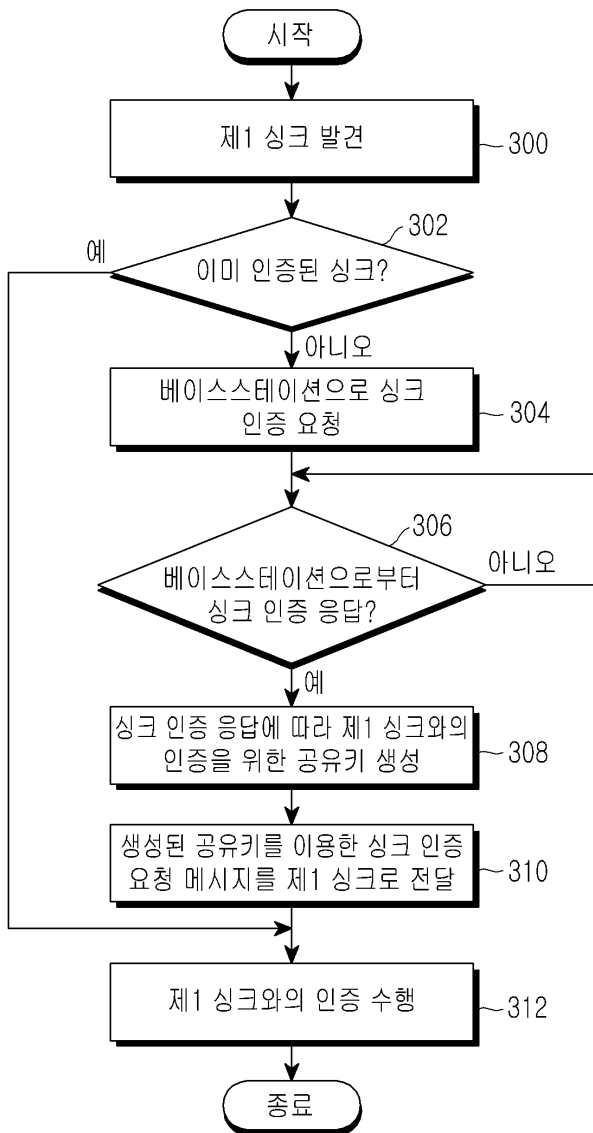
【Drawing 1】



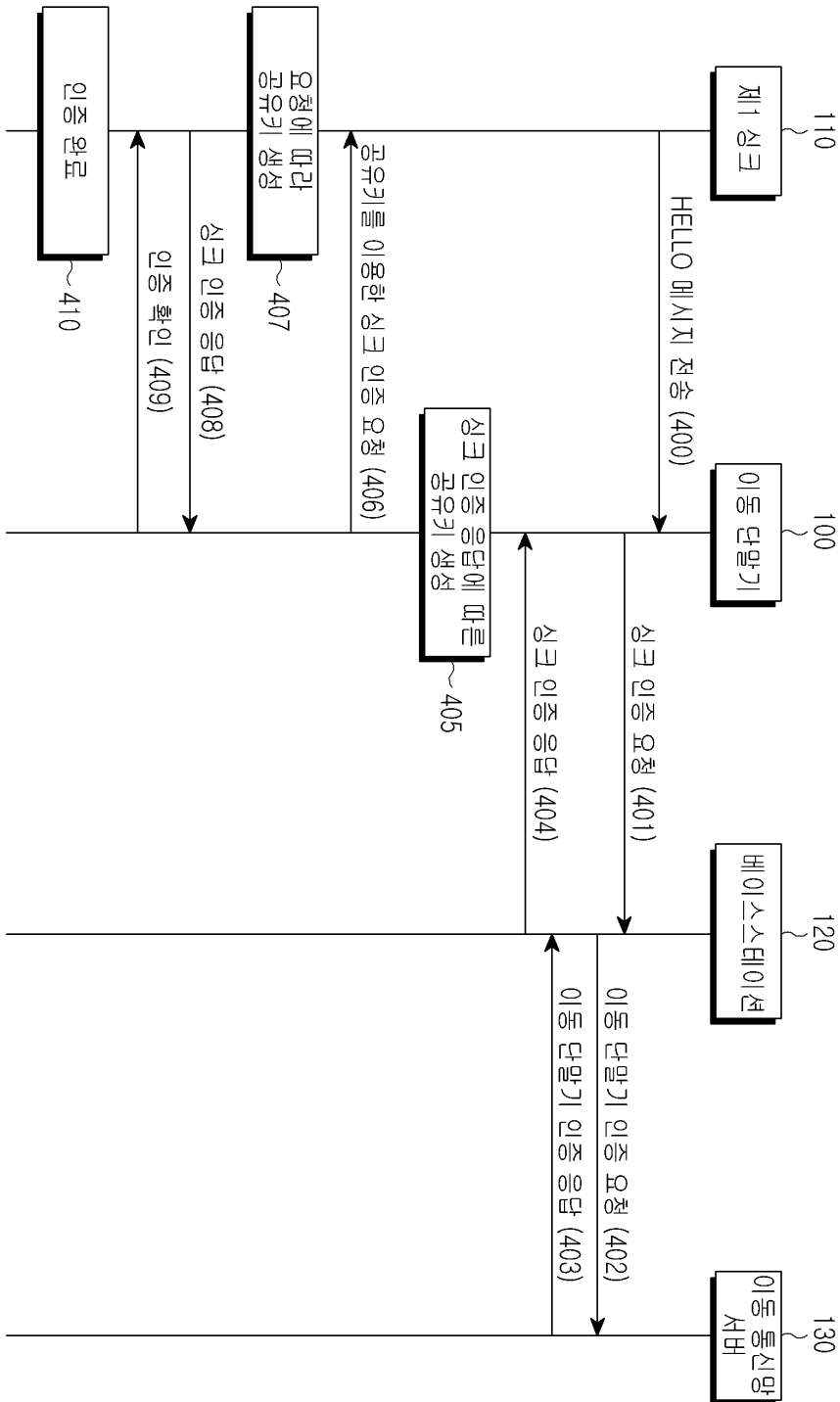
【Drawing 2】



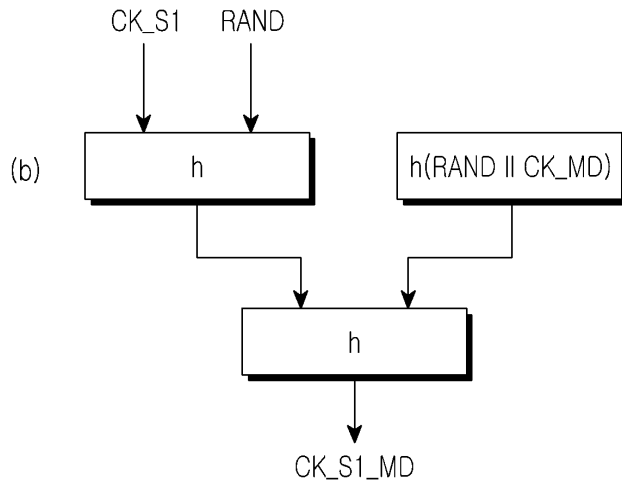
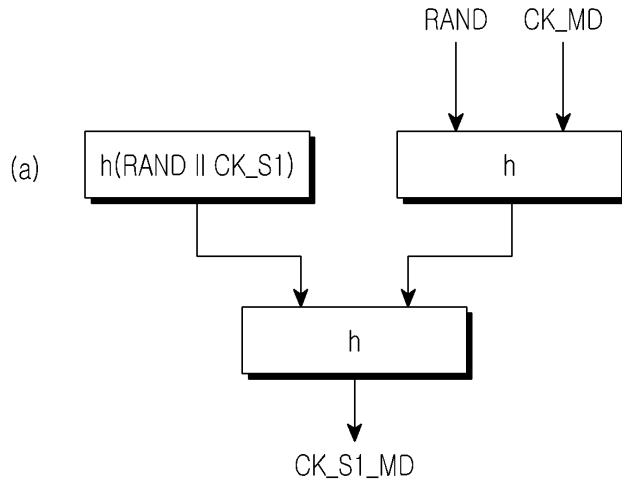
【Drawing 3】



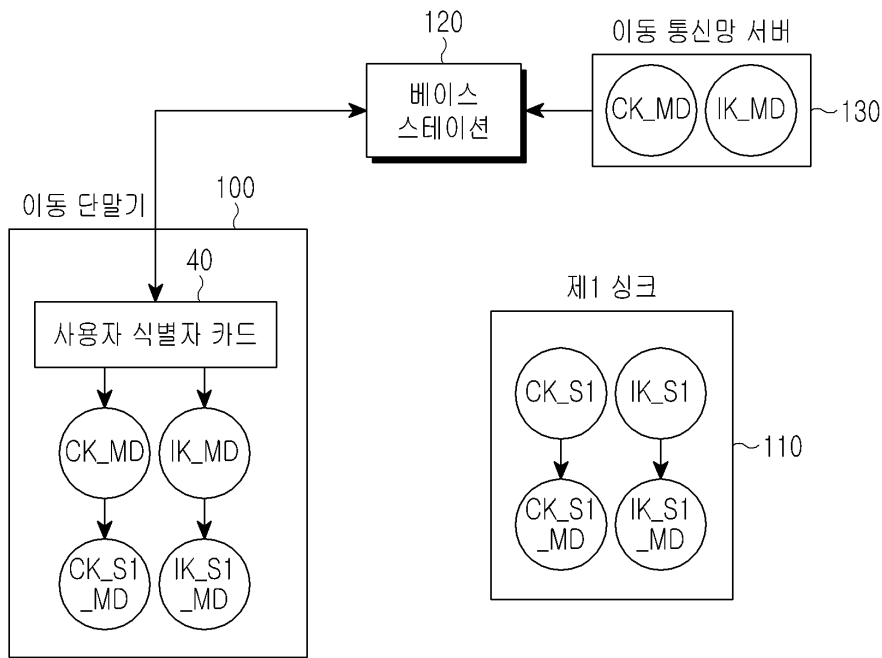
【Drawing 4】



【Drawing 5】



【Drawing 6】





Request for Examination

【Classification】 examination request

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Submitter】

【Organization Name】 Korea Advanced Institute of Science and Technology

【Patent Customer Number】 3 -1 99 8- 0 9 88 66 -1

【Relation with a case】 application person

【Agent】

【Name】 LEE, Keon Joo

【Agent's Code】 9 -1 99 8- 000 33 9 -8

【Registration number of general power of attorney】 200 3-00 14 49 -1

【Mark of events】

【Application Number】 10-200 9-0 11 47 25

【Title of Invention】 SYSTEM AND METHOD FOR AUTHENTICATING SINK USING MOBILE NETWORK

【Official Fee】



【Examination Fee】 14 6 90,000 won

【Purport】

I submit it to the head of the Korean Intellectual Property Office as above. Dari in this state (Name or In)

Sending
 number : 9-5-2016-037760927
Dispatche
 d date : 2016.05.24.
Submissio
 n due 2016.07.24.
 date :

YOUR INVENTION PARTNER



Intellectual Property Office

Request for the Submission of an Opinion

Applicant Name a person besides SAMSUNG ELECTRONICS CO., LTD

Address

Agent Name LEE, Keon Joo

Address

Inventor Name SHON, Tae Shik

Address

Inventor Name PARK, Yong Suk

Address

Inventor Name HAN, Kyu Suk

Address

Inventor Name KIM, Kwang Jo

Address

Inventor Name KIM, Jang Seong

Address

Application No 10-2009-0114725

Application date 2009.11.25.

Title of Invention SYSTEM AND METHOD FOR AUTHENTICATING SINK USING MOBILE NETWORK

1. Because of having the reason for refusal like the examination result next about this application and notifying of this according to the article 63 of Patent Act in case it has the opinion or the correction is needed or it wants opinion (the reply, and the Written Reply) to submit the Amendment [form of attached document No.9 of Enforcement Regulation of Patent Act].

2. In the case to extend the submission due date (2016.07.24.), the due date of submission of the can be extended through the request for an extension of designated period to 4 month. In this case, request for the extension has to do by unit of 1 month and 2 month or greater is summed up in the need in the range that does not

exceed 4 month and it can request the extension. The Written Substantiation describing the proprietary is additionally attached in the time for to postponing the designated period to the generation (the guideline reference of the lower part) of the inevitable proprietary in excess of 4 month and request for the extension has to be applied.

[Examination result]

Subject of Claim 1-14
examination claim:

The law articles in connection with the part in which it has the reason for refusal of this application

| Sequence number | The part in which it has the reason for refusal | Related law articles |
|-----------------|---|------------------------------------|
| 1 | Claim 1 to claim 14 | The article 29(2) of Patent Act |
| 2 | Claim 4 to claim 7 | The article 42(4)(2) of Patent Act |

[The detailed reason for refusal]

1. The invention in claim 1 of the patent claim of this application to claim 14 cannot receive patent like the lower part according to the article 29(2) of Patent Act since a person having ordinary skill in the art to which the invention pertains easily can invent before the application.

- Follows -

a. It is formed including the sink in which claim 1 delivers the sink authentication request for the sink and the base station delivering the sink authentication response which contains the sink authentication information about the sink if the system has the sink authentication request about the sink from the mobile terminal to the mobile terminal to the base station using the mobile radio communication network the system for the authentication between the mobile terminal and the sink and authenticated with the mobile terminal and the mobile terminal authenticating the sink using the received sink authentication information if the sink authentication response is received from the base station.

In the meantime, in cited invention (KR10-2007-0112483 A, and 2007.11.26.), the authentication request is received from the authenticator and the authentication request for the applicant and the certificate server transmitting the authentication information the authentication information after doing the production is transmitted and the authentication information is received from the certificate server and it is written about the authenticator authenticating the applicant. Therefore, the normal technical engineer as to claim 1, easily can

invent to the configuration where the base station of claim 1 , and the mobile terminal and sink are corresponded to the certificate server and the authenticator of citation invention and applicant through the cited invention.

- b. It limits that claim 2 further includes the mobile network server to the dependent claim of claim 1. But it is facilitated to analogize this from the certificate server of the cited invention it will do.
- c. Claim 3 through 7 substantially limits to the dependent claim of claim 1 in the mobile terminal, and the base station and mobile network server about the authentication request message, and the transmission of the authentication response. But the normal technical engineer easily can recognize as the flow of the message in which such configuration is exchanged in the authentication procedure with each object and the technical mapping can be recognized from the PMK (pairwise master key) in which about the shared key production for the authentication and authentication execution are written in the cited invention it will do.
- d. In the authentication system in which claim 8 through 11 and 12 through 14 include the mobile terminal, sink, base station, mobile network server, by corresponding to the invention in which the category including the technical mapping written in claim 1 through 7 is different using the mobile radio communication network as the method for the authentication between the mobile terminal and the sink it is facilitated to the reason for being the same to the normal technical engineer.

2. The application cannot be granted for a patent since it cannot satisfy the requisite according to the article 42(4)(2) of Patent Act due to deficiency in the description of claim 4 of the patent claim to claim 7 as pointed out below.

- Follows -

- a. In claim 4 through 7, it is written as "mobile network server". But because the configuration is written in advance it does not have claim 4 of the form through 7 in which the mobile network server quotes claim 3 to the element of claim 2 will do. Therefore the material is not clear. End.

[Appendix]

Appendix 1 10-2007-0112483 A (2007.11.26.) one copy. end.



Written Opinion

【Classification】 Opinions according to notice of grounds for rejection, etc.

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Submitter】

【Organization Name】 Korea Advanced Institute of Science and Technology

【Patent Customer Number】 3 -1 99 8- 0 9 88 66 -1

【Relation with a case】 application person

【Agent】

【Name】 LEE, Keon Joo

【Agent's Code】 9 -1 99 8- 000 33 9 -8

【Registration number of general power of attorney】 200 3-00 14 49 -1

【Mark of events】

【Application Number】 10-200 9-0 11 47 25

【Dispatch number that caused the submission】 9 -5- 20 16 -0 37 7 60 9 -2 7



【Opinion Contents】 like a star

【Purport】

As above, it is submitted to the head of the Intellectual Property Office (the head of the Patent Tribunal, the head of the Tribunal).



Opinion Contents

The applicant's opinion on the reason for the rejection dated May 24, 2016 for Patent Application No. 11 47 25 (hereinafter referred to as the present application) in 2009 is as follows.

- all negative -

1. According to the report on the submission of opinions dated May 24, 2016,

1. The invention described in the claims 1 to 14 of the claims of the present application is unpatentable in accordance with the Patent Act Article 29(2) because it can be readily derived by a person having ordinary skill in the art before the application as follows.

- Ara -

A. Claim 1 pertains to a system for authenticating between a mobile terminal and a sink by using a mobile communication network, and is configured to comprise:

a base station for transmitting, to the mobile terminal, a sink authentication response including sink authentication information for a sink when there is a sink authentication request for the sink from the mobile terminal; and the mobile terminal for transmitting the sink authentication request for the sink to the base station and authenticating the sink by using the received sink authentication information when the sink authentication response is received from the base station, and the sink for authenticating the mobile terminal.

Meanwhile, the cited invention (Published Patent Publication No. 10-200 7-01 12 48 3, 2007 11.2 6. the authentication information is received from the certificate server it transmits the authentication request about the certificate server in which it transmits the authentication information after it receives the authentication request from an authenticator and it produces the authentication information and applicantIt describes the certifier who certifies the high applicant. Therefore, the base station, the mobile terminal, and the sink of the claim 1 correspond to the authentication server, the authenticator, and the

applicant of the cited invention, and thus the claim 1 can be easily derived by a person with ordinary skills in the art through the cited invention.

I. Claim 2, which is dependent on claim 1, delimits the invention wherein a mobile communication network server is further included, but it would be easy to infer this from the authentication server of the cited invention.

All. Claims 3-7, which are substantially dependent on claim 1, delimit the transmission of the authentication request message and the authentication response message in the mobile terminal, the base station, and the mobile communication network server, but the feature could be readily recognized by a person skilled in the art by the flow of the message exchanged with each object in the authentication process, and the generation of the shared key for authentication and the execution of the authentication could be derived by a person skilled in the art from the feature disclosed in the prior art reference of PMK (pairwise master key).

D. Claims 8-11 and 12-14 pertain to a method for authenticating between a mobile terminal and a sink by using a mobile communication network in an authentication system including a mobile terminal, a sink, a base station, and a mobile communication network server, and the category including all the technical ideas set forth in claims 1-7 corresponds to the other invention, and thus claims 8-11 and 12-14 could be readily derived by a person skilled in the art for the same reason.

2. This application is based on the description of claims 4 to 7 of the claims below. As mentioned above, it is unpatentable because it does not meet the requirements of Article 42 (4) 2 of the Patent Act.

- Ara -

A. "Claims 4 to 7 describe "the mobile communication network server", but the mobile communication network server is a component of claim 2, and claims 4 to 7 of the format citing claim 3 do not describe the configuration in advance,

and thus the description is not clear." It's been announced to be rejected for the reason.

2. The present applicant has amended the scope of the claims of the present invention as follows in the letter of amendment submitted to the same person as the opinion letter.

(1) Claim amendment content

A. In order to resolve the grounds for rejection 1 (related to Article 29 (2) of the Patent Act),

The mobile terminal of claim 1, comprising: a communication module for transmitting and receiving messages

Sensor for receiving sync information; and a control unit which transmits a sink authentication request for the sink to a base station together with information indicating that the mobile terminal is authenticated by a mobile communication network server, receives a sink authentication response including sink authentication information for the sink from the base station, and authenticates the sink by using the received sink authentication information.

Correct to .

Claim 8 pertains to a method for authenticating with a sink in a mobile terminal, the movementAn authentication method comprising: transmitting, to a base station, a sync authentication request for a sync together with information indicating that a terminal is authenticated by a mobile communication network server; receiving, from the base station, a sync authentication response including sync authentication information for the sync; and performing authentication with the sync using the received sync authentication information.

It was corrected to .

In addition, claims 2, 7, 9, 13, and 14 have been deleted, and claims 3 to 6 and 11 to 12 have been corrected.



I . It is considered that the reason for rejection 2 (related to Patent Act No. 42 Article 4 No. 2) can be solved together by the above countermeasures.

3. The differences between the present invention and the cited invention are as follows, given the applicant's opinion in detail.

(1) Basic fact

A. gist of the present invention

The gist of the present invention is as set forth in the amended claim 1.

『Claim 1. as to the mobile terminal ,

Communication module for transmitting and receiving messages;

Sensor for receiving sync information;

information indicating that the mobile terminal is authenticated by a

mobile communication network server and a control unit which transmits

a sink authentication request for the sink to a base station, receives a sink

authentication response including sink authentication information for the sink

from the base station, and authenticates the sink by using the received sink

authentication information.

Claims 3-6 , 8 and 11-12 are omitted.

I . The gist of the cited invention (Published Patent Publication No. 10-200 7-01 12 48 3).

in claim 1 of the cited invention

『As a method of providing applicant access to a wireless communication network

The step of receiving a message in authenticator the authentication request from applicant

The step of writing out the state in authenticator based on the authentication request

a step of relaying the authentication request to a basic authenticator, wherein the basic authenticator is connected to an authentication server

relaying authentication information from the basic authenticator to the authenticator, wherein the authentication information is generated in an authentication server

A step for receiving the authentication information from authenticator and
A method comprising the step of fulfilling said authentication request is disclosed.

(2) The comparison between the present invention and the cited invention

A. purpose and effect comparison

The present invention relates to sink authentication using a mobile communication network.

The identification paragraph [000 5] - [000 7] of the present invention is described as follows.

[000 5]: However, since the authentication of the node is requested to the base station whenever the node is connected to the sink, in the case of multiple hops, node information is transmitted to the base station through a plurality of sinks, and authentication information needs to be received from the base station.

[000 6]: In addition, when authentication is performed through the base station in a sensor network in a multi-hop environment, a large number of sinks are required when authentication is performed, and thus a large number of communication overheads occur, and there is a problem in that the sink detection time and the communication overheads may increase exponentially as the number of hops increases.

[000 7]: In addition, when such a node has mobility, there is an increasing need to perform authentication between a moving node and a sink using a mobile communication network in order to perform authentication between the moving node and the sink on a multi-hop sensor network.

That is, the present invention provides a method for performing authentication between a mobile terminal and a sink by using an authentication key generated

in advance through authentication between the mobile terminal and a mobile communication network server by using a mobile communication network.

To this end, the mobile terminal for authentication with a sink in claim 1 Communication module for sending and receiving messages; Sensor for receiving sync information; a sink with information indicating that the mobile terminal is authenticated by a mobile communication network server and a control unit which transmits a sink authentication request for the sink to a base station, receives a sink authentication response including sink authentication information for the sink from the base station, and authenticates the sink by using the received sink authentication information.

Accordingly, according to the present invention, since the mobile terminal transmits the information authenticated by the mobile communication network server to the base station together with the authentication request, the sink authentication information for the sink can be directly received without separately authenticating the mobile terminal.

On the other hand, the cited invention is for providing client access to a communication network through an authenticator in the communication network.

The cited invention is clearly disclosed in 'the claim 1'.

The step of receiving a message in authenticator the authentication request from applicant The step of writing out the state in authenticator based on the authentication request a step of relaying the authentication request to a basic authenticator, wherein the basic authenticator is connected to an authentication server relaying authentication information from the basic authenticator to the authenticator, wherein the authentication information is generated in an authentication server A step for receiving the authentication information from authenticator and a step of performing the authentication request.

Accordingly, the cited invention can provide an improved system and method for providing multi-hop access.

That is, the cited invention is only for providing multi-hop access through an authenticator in a communication network

As in the present invention, the mobile terminal transmits the information authenticated by the mobile communication network server to the base station together with the authentication request, so that the feature for directly receiving the sink authentication information for the sink is not disclosed at all without separately authenticating the mobile terminal.

Therefore, prior art reference does not teach the unique purpose of the present invention and the effects provided by such an authentication method for reducing the time required for authentication and reducing the communication and operation overhead for authentication and key exchange in a sensor network in a multi-hop environment .

I . composition comparison

1) The comparison between the corrected invention of the claim 1 and the cited invention

The invention of claim 1

as to the mobile terminal ,

Communication module for transmitting and receiving messages;

Sensor for receiving sync information;

a sink authentication response which transmits a sink authentication request

for the sink together with information indicating that the mobile terminal is

authenticated by a mobile communication network server to a base station

and includes sink authentication information for the sink from the base

station and a control unit for authenticating the sink by using the received sink

authentication information.

Accordingly, according to the present invention, since the mobile terminal transmits the information authenticated by the mobile communication network server to the base station together with the authentication request, the sink authentication information for the sink can be directly received without separately authenticating the mobile terminal.

The invention as in claim 1 is characterized by a control unit for transmitting a sync authentication request for the sync to a base station together with information indicating that the mobile terminal is authenticated by a mobile communication network server, receiving a sync authentication response including sync authentication information for the sync from the base station, and authenticating the sync by using the received sync authentication information.

It is considered that this feature is not disclosed in the cited invention.

The detailed description of the present invention is described as follows.

[00 51] The mobile terminal 100 generates a sink authentication request message for requesting authentication of the first sink from the base station 120 in step 1 of the sink instant noodle 40 in which the first sink 110 is not authenticated. Then, the mobile terminal 100 generates authentication information $u[1]=enc\{CK_MD, S1||u[0]||v[0]\}$ obtained by encrypting $S1$, $u[0]$, and $v[0]$ with an encryption key CK_MD shared between the base station 120 and the mobile terminal 100, and generates integrity information $v[1]=MAC\{IK_MD, MD|BS||S1||APP_REQ||u[1]\}$ for integrity checking of $u[1]$. Here, IK_MD denotes an integrity check key shared between the base station 120 and the mobile terminal 100. Moreover, passwordKey C K_MD and integrity keyI Kof the mobile communications network server(130) and the mobile terminal(100) in which MD is performed before 40 1 stepGBAbootstrap ping(B o o t s t r a p i n g) Generate through operationIt becomes. At this time, the , G BA boot string wrapping operation uses the user identification card(40)the mobile terminal(100)

and mobile radio communications network between servers (130) the shared key is produced each other the operation performing authentication It means .

Thereafter, the mobile terminal 100 requests sync authentication while transferring the ID MD, $u[1]$, and $v[1]$ of the mobile terminal 100 to the base station 120 together with the generated sync authentication request message.

[0053] The base station 120 receiving the request checks the received ID of the mobile terminal 100 to determine whether the mobile terminal 100 requesting sync authentication is an already authenticated mobile terminal. As a result of the determination, when the mobile terminal is not authenticated, the base station 120 requests authentication of the mobile terminal 100 from the mobile communication network server 130 in step 402.

In step 403, the mobile communication network server 130 transmits a mobile terminal authentication response message including an encryption key and an integrity key of the mobile terminal 100 shared in advance to the base station 120 through a G BA operation such as 3G PP TS 33 .2 20.

[0055] 40 In step 4 **The base station (120) uses the received encryption key and integrity key of the mobile terminal (100) to be first sink (110) for authentication sink Generate a sync authentication response message including authentication information and transmit it to the mobile terminal (100)** It does.

According to the above, when the mobile terminal transmits the sync authentication request message to the base station, the mobile terminal transmits the sync authentication request message including information indicating that the mobile terminal is the mobile terminal authenticated by the mobile communication network server to the base station.

When the mobile terminal is an authenticated mobile terminal, the base station generates a sync authentication response message including sync authentication information and transmits the sync authentication response message to the mobile terminal.

In other words, the mobile terminal of the present invention transmits information indicating that the mobile terminal is authenticated by the mobile communication network server to the base station, so that a sink authentication response including sink authentication information can be received without separately performing authentication for the mobile terminal. On the other hand, paragraphs [0026]–[0027] of the cited invention are disclosed as follows.

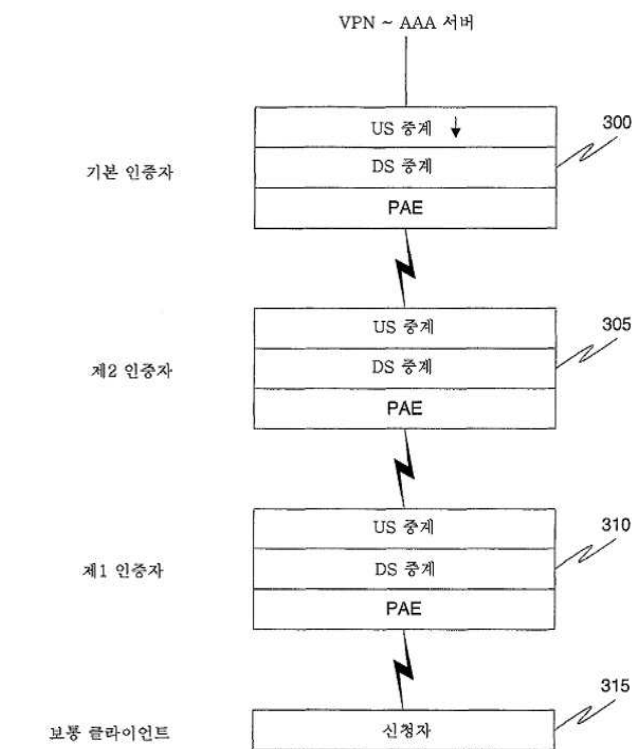


FIG. 3 of the cited invention

FIG. 3 illustrates a method in which authentication using a relay process is provided. According to one embodiment, the downstream relay is an in-bound relay when the lower nodes in the relay transmit the authentication message received from the applicant 315 to the basic authenticator 300. Normally, a client-in applicant has a first authentication message to the authenticator(310)It sends. The authenticator is an applicant who has an indirect security relationship with the authentication server through the basic authenticator 300. As shown in FIG. 3, firstthe authenticator(310)secondan authenticator

(305)certified through Accordingly, it has a security relationship with the authentication server through the second authenticator 305 and the basic authenticator 300. The applicant 315 first sends an authentication request to the first authenticator 310. The authentication request relayed between the first authenticator 310 and the basic authenticator 300 may be performed using various methods. As mentioned above, the authentication request is a RADIUS (Remote Authentication Dial In User Service) message, EAPOL (extensible) It can be transmitted as a authentication indication packet over LAN) origination message, or as another similar authentication protocol. According to an EAPOL embodiment, the authentication request involves the use of a WDS frame format integrated within the EAPOL message. The WDS frame adds the source address, destination address, transmission address and receiver address to packet. The first authenticator 310 receives an authentication request, such as an EAPOL initiation message, and writes a state. The state is made of information including a source address, a destination address, a transmission address and a receiver address. In the embodiment shown in FIG. 3, the state generated by the first authenticator 310 includes a source address and a transmission address as the address of the applicant. Then, the EAPOL packet is relayed to the next hop in the downstream relay chain.**second authentication The ruler(305) is the first from authenticator(310) the authentication request is received.** The source address is the applicant's address; When the transmission address is the address of the first authenticator 310, the second authenticator 305 also creates a state. As used herein, the state includes one element (element) of the status address pairing table, the element pairing each source address with a transmitter address. The status establishes a relationship when the second authenticator knows the node that has sent the applicant's authentication request to the second authenticator 305. This relationship may be used to relay authentication information received

from an authentication server to an applicant through a basic authenticator. The authentication request reaches the basic authenticator 300 when the basic authenticator creates a state. The source address is an address of the applicant and the transmission address is an address of the second authenticator 305. Then, **The authentication request is forwarded to the authentication server for confirmation (valid identification)**. As mentioned above, the basic authenticator 300 is virtual. A private network or similar security connection is used to have a permanent security relationship with the authentication server.

[0027] As used herein, the up-stream relay is an out-bound relay furnace, wherein **the authentication information received from the certificate server certifier is again relayed**. As shown in FIG. 3, the basic authenticator 300 relays the authentication information received from the authentication server to the next hop, that is, the second authenticator 305 by using the state created in the in-bound relay. As in the above-described example, the second authenticator 305 receives the E AP OL packet from the basic authenticator 300 and creates an additional state when authentication information is stored. The authentication information includes a unique PM K (unique pairwise master key) corresponding to the applicant, timer, and other information. **second the authenticator (305) in-bound the first authenticator is distinguished as the node relaying the authentication request in relay and the authentication information is therefore the first to the authenticator (310) it relays. second certifier** Firstly, in the , **authentication information, the destination address is determined and the authentication information is transmitted certifier discriminate** . Subsequently, the second authenticator searches the status address pairing table. In one embodiment, the status address pairing table is created by inbound authentication requests. The second authenticator searches for an element having a matching source address in the status address pairing table. When the source address is found, the second authenticator finds the initially extracted



paired transmitter address from the same in-variant authentication request information. If the source address and the transmitter address of the in-bound authentication request are identified in the status address pairing table, the second authenticator uses the source address as the destination address for the out-bound authentication information packet and the transmitter address as the receiver. It's used as de-res. Similarly, the first authenticator 310 receives the E AP OL packet from the second authenticator 305, creates an additional state, and identifies the applicant as the next node in the relay. In this case, authentication information including PM (pairwise master) is not transmitted to the applicant. The first authenticator 310 uses this PM K to authenticate the applicant by the 4-way handshake. 4-direction handshake process **a first key generated by the applicant and from the authentication server in the authenticator(310) Applicant is certified by using the unique key received by.** However, those skilled in the art will appreciate that other methods may be used to create a state that enables the relay process and identify the relay node through which the applicant can establish a secure connection to the authentication server, and these methods are within the scope of the present invention.

According to the above, the prior art reference transmits an authentication request to an authentication server through a first authenticator, a second authenticator, and a basic authenticator in order to authenticate an applicant, and authentication information received from the authentication server is transmitted to the basic authenticator, the second authenticator, and the first authenticator, and the first authenticator authenticates the applicant by using the authentication information.

In other words, the cited invention only discloses that the first authenticator must be authenticated by the second authenticator and the second

authenticator must be authenticated by the basic authenticator in order to authenticate the applicant.

As in the present invention, since the mobile terminal transmits information indicating that the mobile terminal is authenticated by the mobile communication network server to the base station, it fails to initiate receiving a sync authentication response including sync authentication information without separately performing authentication for the mobile terminal.

That is, since the cited invention requests and receives authentication information for an applicant from an authentication server through multiple certifiers, each certifier must be authenticated, and an authentication request for the applicant must be delivered.

According to the present invention, since sink authentication information for a sink is directly received without separately authenticating a mobile terminal, it is possible to reduce communication and calculation overhead for authentication and key exchange in a sensor network in a multi-hop environment, and to reduce time required for authentication.

In addition, since the corrected claim 8 corresponds to the claim 1, the claim 8 has the same differences as the claim 1.

2) Comparison between the dependent inventions and the cited invention
Claims 3 to 6 are dependent inventions of claim 1 and claims 10 to 12 are dependent inventions of claim 8.

Each of claims 3 to 6 and 10 to 12 has the same differences as those described in claims 1 and 8.

(3) Conclusion

As described above, the present invention and the cited invention adopt completely different purposes, configurations, and effects. It's there.



Therefore, the present invention can not be easily invented by a person having ordinary skill in the art of the invention by using the cited invention when the present application is filed.

4. Accordingly, it is believed that the present invention does not violate Article 29 (2) and Article 42 (4) 2 of the Patent Act, so please take the above opinion into account at the time of re-examination and make a decision on the patent.



Amendment to Bibliographic Information

【Classification】 specification etc. correction

【Submitter】 patent office field

【Submitter】

【Organization Name】 SAMSUNG ELECTRONICS CO., LTD.

【Patent Customer Number】 1-1 99 8 -10 4 27 1-3

【Relation with a case】 application person

【Submitter】

【Organization Name】 Korea Advanced Institute of Science and Technology

【Patent Customer Number】 3 -1 99 8- 0 9 88 66 -1

【Relation with a case】 application person

【Agent】

【Name】 LEE, Keon Joo

【Agent's Code】 9 -1 99 8- 000 33 9 -8

【Registration number of general power of attorney】 200 3-00 14 49 -1

【Mark of events】

【Application Number】 10-200 9-0 11 47 25



【Dispatch number that caused the submission】 9 -5- 20 16 -0 37 7 60 9 -2 7

【Documents to be corrected】 specification etc

【What to correct】

【Items to be corrected】 like a star

【Correction method】 like a star

【Correction contents】 like a star

【Purport】

As above, it is submitted to the head of the Intellectual Property Office (the head of the Patent Tribunal, the head of the Tribunal).

【Official Fee】

【Amendment Fee】 4,000,000 won

【Additional fees for examination requests】 0 won

【Other fees】 0 won

【Total】 4,000,000 won



Amendment

【Correction item】 Claim 1

【Correction method】 Change

【Correction content】

【Claim 1】

as to the mobile terminal ,

Communication module for transmitting and receiving messages;

Sensor for receiving sync information;

and a control unit which transmits a sink authentication request for the sink to a base station together with information indicating that the mobile terminal is authenticated by a mobile communication network server, receives a sink authentication response including sink authentication information for the sink from the base station, and authenticates the sink by using the received sink authentication information.

【Correction item】 Claim 2

【Correction method】 Delete

【Correction item】 Claim 3

【Correction method】 Change

【Correction content】

【Claim 3】

The method of claim 1, wherein the control unit is

When there is a request for authenticating the sink, it is determined whether the sink is an already authenticated sink, and when it is determined that the sink is an unauthenticated sink, a sink authentication request message for the sink is transmitted to the base station.



【Correction item】 Claim 4

【Correction method】 Change

【Correction content】

【Claim 4】

The method of claim 1, wherein the control unit is

When there is a request for authenticating the sink, it is determined whether the sink is an already authenticated sink, and when the sink is identified as an authenticated sink, mutual authentication is performed using a shared key generated through the sink.

【Correction item】 Claim 5

【Correction method】 Change

【Correction content】

【Claim 5】

The method of claim 1, wherein the control unit is

a mobile terminal which generates a shared key by using sink authentication information received from the base station and transmits a sink authentication request including shared key generation information for the generated shared key to the sink.

【Correction item】 Claim 6

【Correction method】 Change

【Correction content】

【Claim 6】

The method of claim 5, wherein the control unit is

When a response to the sink authentication request is received from the sink, authentication with the sink is completed.



【Correction item】 Claim 7

【Correction method】 Delete

【Correction item】 Claim 8

【Correction method】 Change

【Correction content】

【Claim 8】

as to the authentication method with sink in the mobile terminal

A process of transferring to the base station the sink authentication request about sink along with the information which shows that the mobile terminal is authenticated with the mobile communications network server

The process of receiving the sink authentication response including the sink authentication information about sink from the base station

and a step of performing authentication with the sink by using the received sink authentication information.

【Correction item】 Claim 9

【Correction method】 Delete

【Correction item】 Claim 10

【Correction method】 Change

【Correction content】

【Claim 10】

The method of claim 8,

a step of determining whether the sink is an already authenticated sink if there is a request for authenticating the sink

The authentication method further includes performing mutual authentication using a shared key generated through the sink when the sink

is identified as an authenticated sink.

【Correction item】 Claim 11

【Correction method】 Change

【Correction content】

【Claim 11】

The method of claim 8, wherein the authenticating of the sink comprises:
a step of generating a shared key by using the sink authentication
information received from the base station
and a process of transferring a sync authentication request including shared
key generation information for the generated shared key to the sync.

【Correction item】 Claim 12

【Correction method】 Change

【Correction content】

【Claim 12】

The method of claim 11, wherein the step of authenticating the sink
comprises:
and a step of completing authentication with the sink when a response to the
sink authentication request is received from the sink.

【Correction item】 Claim 13

【Correction method】 Delete

【Correction item】 Claim 14

【Correction method】 Delete

