US 20120226909A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2012/0226909 A1

(43) Pub. Date: Sep. 6, 2012

Lucidarme

(54) METHOD OF CONFIGURING A NODE, RELATED NODE AND CONFIGURATION SERVER

(75) Inventor: **Thierry Lucidarme**, Montigny-le-Bretonneux (FR)

(73) Assignee: **ROCKSTAR BIDCO LP**, New York, NY (US)

(21) Appl. No.: **13/469,662**

(22) Filed: **May 11, 2012**

Related U.S. Application Data

(63) Continuation of application No. 11/582,683, filed on Oct. 18, 2006, now Pat. No. 8,200,967.

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

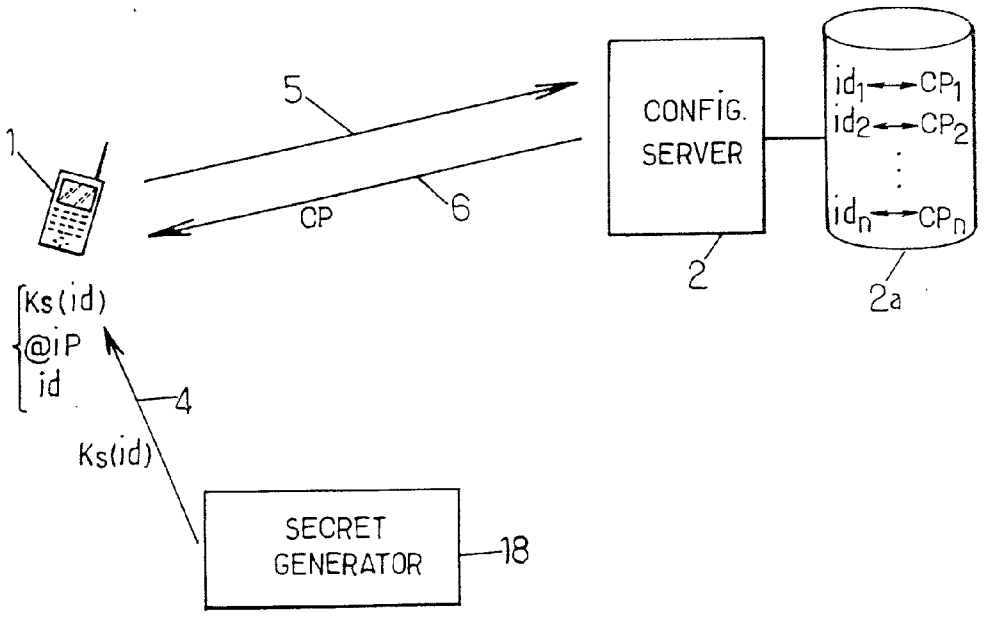
(52) **U.S. Cl.** **713/171**; 713/168

(57) **ABSTRACT**

A method for configuring a node, said node holding a public key depending on an identifier relating to said node, a related secret key and an address of a configuration server storing sets of configuration parameters for respective nodes, the method comprising the following steps carried out at the configuration server:

identifying said node by use of an identity based identification algorithm taking account of said public and secret keys; and

when said node has been successfully identified, retrieving the set of configuration parameters stored for said node and transmitting said set of configuration parameters to said node.



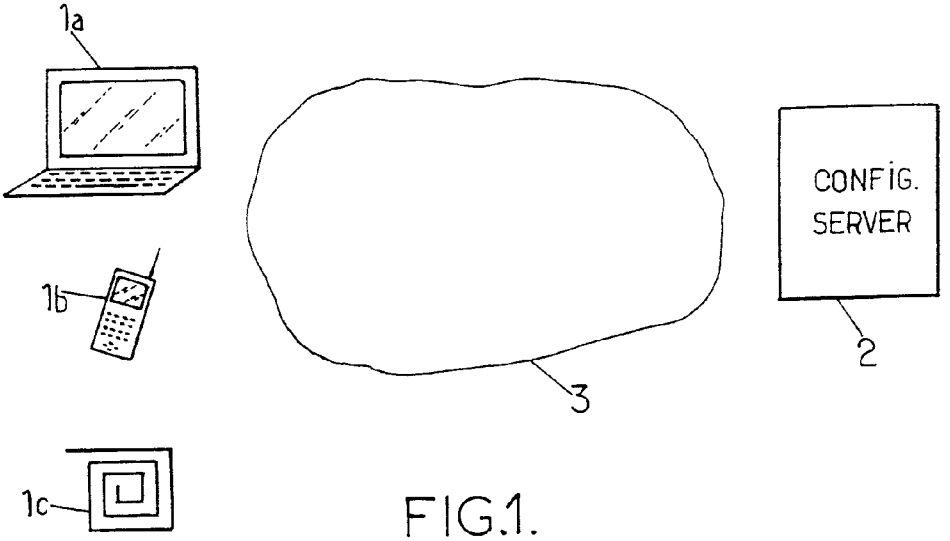

1a
1b
1c
CONFIG.
SERVER
2
3

FIG.1.

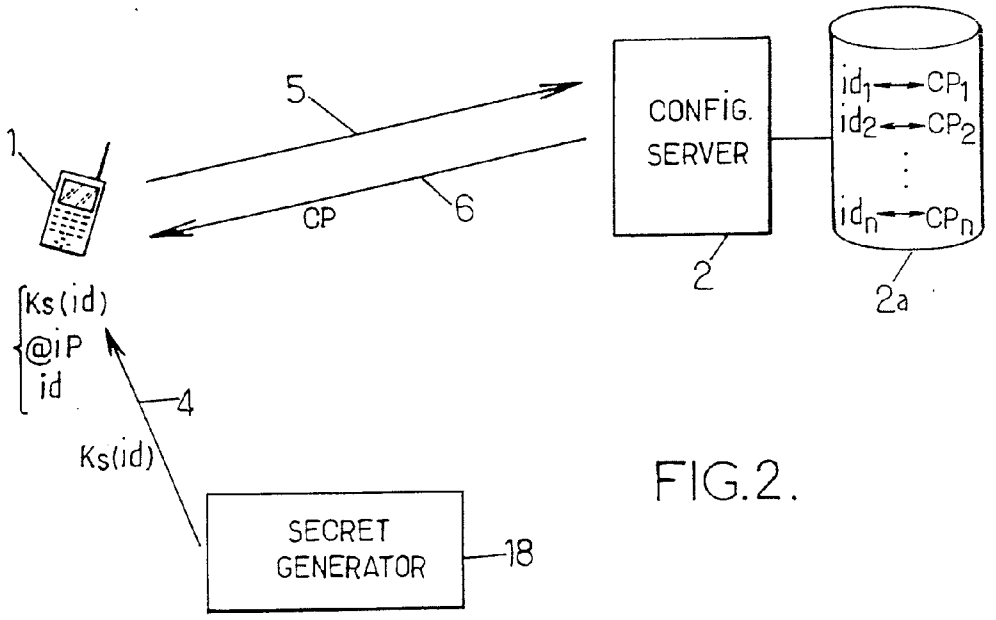

1
5
CP
6
CONFIG.
SERVER
2
id1 CP1
id2 CP2
idn CPn
2a
Ks(id)
@iP
id
4
Ks(id)
SECRET
GENERATOR
18

FIG.2.

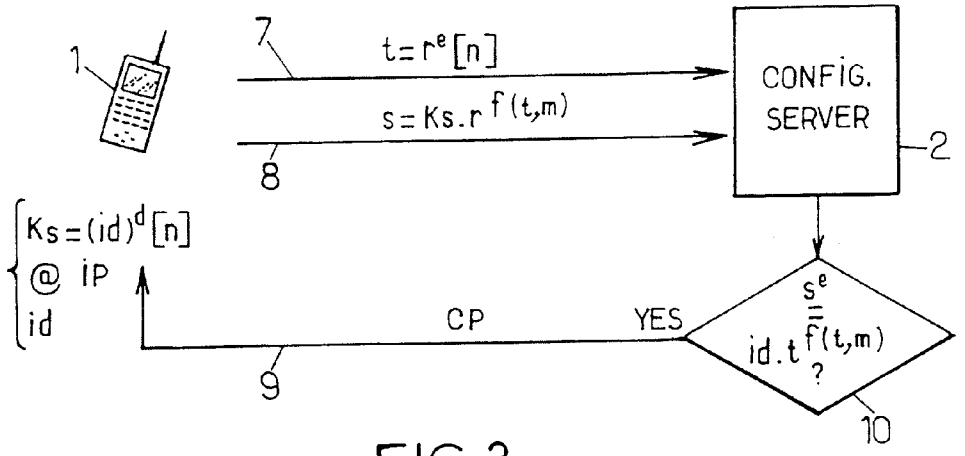

1
7
t=r^e[n]
s=Ks.r^f(t,m)
8
CONFIG. SERVER
2
Ks=(id)^d[n]
@ IP
id
CP
YES
s^e = id.t^f(t,m) ?
9
10

FIG.3

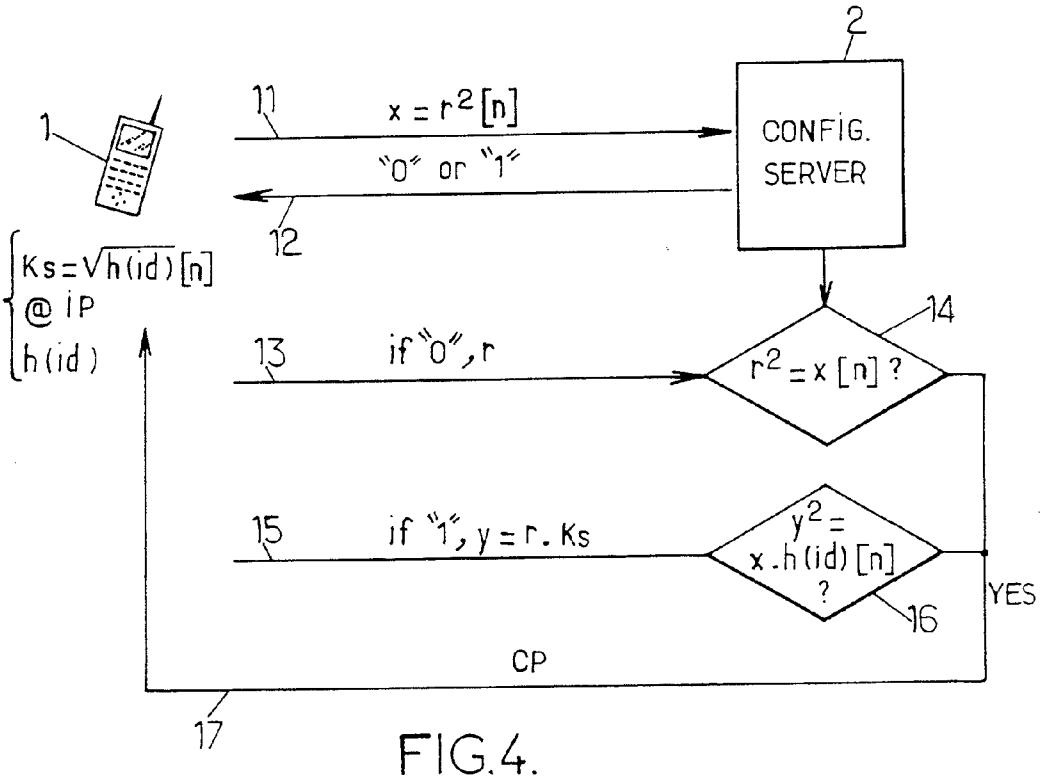

2
1
11
x=r^2[n]
"0" or "1"
12
CONFIG. SERVER
Ks=√h(id)[n]
@ IP
h(id)
13
if "0", r
14
r^2=x[n] ?
15
if "1", y=r.Ks
y^2 = x.h(id)[n] ?
16
YES
CP
17

FIG.4.

METHOD OF CONFIGURING A NODE, RELATED NODE AND CONFIGURATION SERVER

BACKGROUND OF THE INVENTION

[0001] The present invention relates to node configuration.

[0002] The term 'node' is to be understood here as any device or system capable of communicating with at least another node. It includes very basic chip cards, RFID (Radio Frequency Identification Chip) tags, sensors, mobile phones, PDAs (Personal Digital Assistants), base stations, servers, gateways, or even whole telecommunication networks. As a non-limiting example, a node may be an access point of an Ambient Network.

[0003] In order to be able to interact with its environment, a node requires some configuration. Of course, such configuration may differ depending on the nature of the node. But it can also depend on the variety of possible environments the node can meet. The environment may even vary in time, especially as far as mobile nodes moving in a radio environment are concerned.

[0004] Bandwidth, power, IP versions, IP addresses, security keys, proxy server addresses are some examples of configuration parameters an update version of which a node should be aware in order to communicate.

[0005] Due to the above mentioned multiplicity of nodes and environments, it is not easy to store relevant and appropriate configuration parameters in any node once and for all when building it.

[0006] Therefore, there is a need for providing any kind of node with relevant and appropriate configuration parameters.

SUMMARY OF THE INVENTION

[0007] The invention proposes a method for configuring a node, said node holding a public key depending on an identifier relating to said node, a related secret key and an address of a configuration server storing sets of configuration parameters for respective nodes, the method comprising the following steps carried out at the configuration server:

[0008] identifying said node by use of an identity based identification algorithm taking account of said public and secret keys; and

[0009] when said node has been successfully identified, retrieving the set of configuration parameters stored for said node and transmitting said set of configuration parameters to said node.

[0010] In this way, the node does not have to store much information or very specific information initially, since only a public key, a secret key and an address of a configuration server are needed. Moreover, due to the fact that the public key depends on said identifier, the stored information is particularly light, by contrast with traditional X.509 certificates for instance. The configuration parameters can also be obtained at any time by the node after a simple identification by the configuration server. Updated versions of configuration parameters can thus be obtained quite easily.

[0011] The invention also proposes a node holding a public key depending on an identifier relating to said node, a related secret key and an address of a configuration server storing sets of configuration parameters for respective nodes, said node comprising:

[0012] means for being identified by the configuration server by use of an identity based identification algorithm taking account of said public and secret keys;

[0013] means for receiving a set of configuration parameters from the configuration server when said node has been successfully identified.

[0014] The invention also proposes a configuration server storing sets of configuration parameters for respective nodes each holding a respective public key depending on a respective identifier relating to said node, a respective related secret key and an address of the configuration server, said configuration server comprising in relation with any one of said nodes:

[0015] means for identifying said node by use of an identity based identification algorithm taking account of a said public and secret keys relating to said node; and

[0016] means for retrieving the set of configuration parameters stored for said node and means for transmitting said set of configuration parameters to said node when means for identifying have successfully identified said node.

[0017] The preferred features of the above aspects which are indicated by the dependent claims may be combined as appropriate, and may be combined with any of the above aspects of the invention, as would be apparent to a person skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIG. **1** is a schematic view of a system implementing the invention;

[0019] FIG. **2** is a schematic view of main exchanges between a node and a configuration server according to the invention;

[0020] FIG. **3** is a first example of configuration using the Shamir's identity-based identification algorithm; and

[0021] FIG. **4** is a second example of configuration using the Fischer-Micali-Rackoff's identity-based identification algorithm.

DESCRIPTION OF PREFERRED EMBODIMENTS

[0022] FIG. **1** shows a computer device **1***a*, a mobile phone **1***b* and a RFID tag **1***c* which form respective nodes, which may be part of an Ambient network for instance.

[0023] As will be explained in more detail below, each one of these nodes holds minimum required parameters for configuration purposes.

[0024] FIG. **1** also shows a configuration server **2** which contains configuration parameters for different nodes, including the nodes **1***a*, **1***b* and **1***c*.

[0025] In the present invention, the nodes **1***a*, **1***b* and **1***c* receive relevant and appropriate configuration parameters from the configuration server **2**, possibly through a communication network **3** which may contain other nodes.

[0026] Since the nodes **1***a*, **1***b* and **1***c* get respective configuration parameters from the configuration server **2**, they can contain very few information initially. This may be advantageous when building such nodes. It also allows the nodes to get updated configuration parameters when needed, e.g. when moving inside a radio environment.

[0027] FIG. **2** shows in more detail how a node can get configured according to an embodiment of the present invention. In this figure, a node **1**, namely a mobile phone, is to be configured.

[0028] Initially, i.e. right after being built and sold to its user, the node **1** may hold only three parameters: an identifier (id in FIG. **2**) relating to the node **1**, i.e. which identifies either the node itself or its user and which may be used as a public key for the node **1** as will be explained below, a function of said identifier (Ks(id) in FIG. **2**) which may be used as a secret key for the node **1** as will be explained below and an address of the configuration server **2**, e.g. an IP address (@IP in FIG. **2**).

[0029] As a variant, a one way function h of the identifier id (h(id)) may be held by the node **1** instead of the identifier id itself. This one way function may be a hash function, such as SHA-1 (specified in the "Secure Hash Signature Standard (SHS)" by the NIST (see FIPS PUB 180-2)) or MD5 (see Request For Comments 1319-121 published by the Internet Engineering Task Force (IETF)) for instance. Of course, other one way functions may suit as well.

[0030] Advantageously, said identifier id is unique for each node and/or user. It can explicitly define the node and/or user. As a non-limiting example, the identifier id may include the following string: firstname.surname.city@domainname.

[0031] Alternatively, the identifier may include an identifier used for other purposes. For instance, when the routing protocol used between the node and configuration server is IP (Internet Protocol) and the allocation of IP addresses is fixed, the identifier id may include the IP address of the node.

[0032] Likewise, when the node is a mobile phone for instance, it is coupled to a SIM (Subscriber Identity Module) card characterizing the user of the mobile phone. The SIM card contains a user identity called IMSI (International Mobile Subscriber Identity), which could be included in the identifier id for configuration purposes according to the invention.

[0033] Although the node **1** may hold the three above mentioned parameters only, it may also hold additional parameters. However, it will be understood that most or all the configuration parameters intended to be used by the node **1** (e.g. bandwidth, power, IP versions, IP addresses, security keys, proxy server addresses, etc.) are not stored in said node initially.

[0034] The secret key Ks(id) may be provided to the node **1** in many different ways. In the example illustrated in FIG. **2**, a secret generator **18** is the entity that generates Ks(id) by applying a trapdoor function to the identifier id (or h(id)) relating to the node **1**. The secret generator **18** then sends the secret key generated to the node **1** (step **4**).

[0035] On the other hand, the configuration server **2** has access to a database **2***a* which may be internal or external. This database **2***a* stores sets of configuration parameters CP_1, CP_2, . . . ,CP_n for respective nodes identified by id_1,id_2, . . . ,id_n respectively.

[0036] In step **5**, the configuration server **2** identifies the node **1** by use of an identity based identification algorithm. This identification step may be requested by the node **1**. During this step, the node **1** and the configuration server **2** exchange messages. Messages can be sent from the node **1** to the configuration server **2** due to the fact that the node **1** knows the address @IP of the configuration server **2**.

[0037] Non-limiting examples of identity based identification algorithms will be described below with reference to FIGS. **3** and **4**. The particularity of such algorithms is that they take account of a public key which depends on an identifier relating to the entity to be identified. They also take account of a related secret key also depending on said identifier, since the secret key derives from the public key by use of a trapdoor function.

[0038] At the beginning of the identification step **5**, the node **1** sends its identifier id (or h(id)) to the configuration server **2**. The configuration server **2** then authenticates whether or not the node **1** is really the one with said identifier id.

[0039] When the configuration server **2** has successfully identified the node **1**, it is capable of retrieving the corresponding set of configuration parameters CP in the database **2***a*, from the identifier id (or h(id)). It can then transmit CP to the node **1** (step **6**). As mentioned above, the identifier id may include a routing address such as the IP address of the node, which allows CP to be sent from the configuration server **2** to the node **1**. In this way, the node **1** finally holds the needed configuration parameters, which makes it able to communicate properly with other nodes.

[0040] The transmission of the configuration parameters CP from the configuration server **2** to the node **1** may be carried out in clear or in an encrypted way. The encryption can be performed in different ways. A first possibility is to establish a secure tunnel between the configuration server **2** and the node **1** as well known. A second possibility is to use an identity based encryption algorithm, such as the Cocks' algorithm described in the article "An Identity Based Encryption Scheme Based on Quadratic Residues", Cryptography and Coding, 8th IMA International Conference, 2001, pp360-363, or the Boneh-Franklin's algorithm "Identity-Based Encryption from the Weil Pairing", Advances in Cryptology—Proceedings of CRYPTO 2001 (2001).

[0041] When using an identity based encryption algorithm, the configuration server **2** encrypts the transmission of CP with a public key which may be different from the one used to identify the node **1**. Typically, this second public key may use a hash function h' different from h. The second public key may also depend on an identifier of the configuration server **2** in addition or in replacement of the identifier id relating to the node **1**. In this case, the node **1** should further hold a second secret key initially in order to decrypt the messages received from the configuration server **2**.

[0042] It should be noted that the use of an identity based identification algorithm to identify the node is really advantageous, because some nodes may have very low power/memory which might prevent them from embedding a heavy X.509 certificate traditionally used for identification or authentication purposes. The heavy PKI (Public Key Infrastructure) infrastructure is also avoided. Moreover, the exchanges between the node and the configuration server are quite light and thus compatible with low bandwidth systems.

[0043] FIG. **3** shows an example of configuration of a node **1** including an identity-based identification using the Shamir's algorithm described in "Identity-based cryptosystems and signature schemes", Proceedings of CRYPTO'84, LNCS 196, page 47-53, Springer-Verlag, 1984.

[0044] In this example, the public key for the node **1** includes the identifier id. Advantageously, the public key may also incorporate other information, such as an expiry date for configuring the node **1**, in which case the configuration parameters may be sent to the node **1** only if the current date

is no later than this expiry date. This public key is id sent to the configuration server **2** by the node **1**.

[0045] Moreover, the node **1** has been provided with $Ks=(id)^d[n]$ as a secret key, where [·] designates the modulo operation, n=p·q, p and q being two long prime integers and d is an integer such that ed=1 [(p−1)(q−1)], e being another integer. While e and n are public, p and q are not (i.e. the factorization of n is not public).

[0046] The node **1** generates a random number r and calculates $t=r^e[n]$ and $s=Ks\cdot r^{f(t,m)}[n]$, where f is a one way function which may be the above mentioned function h, e.g. a hash function such as SHA-1 or MD5, and m is a known message. Advantageously, m can be set to id. The node **1** then sends t and s to the configuration server **2** (steps **7** and **8**).

[0047] The configuration server **2** calculates $s^e=(Ks)^e\cdot r^{e\cdot f(t,m)}[n]$ and checks whether it equals $id\cdot t^{f(t,m)}[n]$. If the check is positive, the configuration server **2** concludes that the node **1** is really the one relating to the identifier id, which means that the node **1** has been successfully identified. The configuration server **2** can then retrieve the configuration parameters CP corresponding to this id and return them to the node **1** (step **9**).

[0048] FIG. **4** shows another example of configuration of a node **1** including an identity-based identification using the Fischer-Micali-Rackoff's algorithm described in "A secure protocol for the oblivious transfer", 1984, presented at EuroCrypt 84.

[0049] The node **1** holds h(id) as a public key and sends it (or id) to the configuration server **2**. Like in the previous example, the public key may also incorporate other information, such as an expiry date for configuring the node **1**.

[0050] The node **1** also holds, as a secret key, $Ks=\sqrt{\sqrt{h(id)}}[n]$, where n=p·q, p and q being two secret long primes. Although h(id) is public, a third party cannot easily obtain Ks, since the calculation of the square root requires to know the factorization of n (Chinese remainder theorem).

[0051] The node **1** chooses a random number r, calculates $x=r^2[n]$ and sends x to the configuration server **2** (step **11**). The configuration server **2** returns a challenge "0" or "1" to the node **1** (step **12**).

[0052] If "0" is received by the node **1**, the latter sends r to the configuration server **2** (step **13**). In this case, the configuration server **2** calculates r^2 and checks whether this equals x[n] (step **14**).

[0053] If "1" is received by the node **1**, the latter sends y=r·Ks to the configuration server **2** (step **15**). In this case, the configuration server **2** calculates y^2 and checks whether this equals x·h(id)[n] (step **16**), which is possible because the public key h(id) is known to the configuration server **2**. If the check is positive, which means that the node **1** has been successfully identified, the configuration server **2** retrieves the configuration parameters CP corresponding to id and return them to the node **1**.

[0054] A sequence including successive challenges "0" or "1" (e.g. one "0" and then one "1") may advantageously be transmitted to the node **1** by the configuration server **2**, before the latter transmits the relevant configuration parameters CP to the node **1**.

[0055] In a non-limiting example of application of the present invention, the node to be configured may be a home gateway (HGW). A HGW provides a radio interface similar to that of a cellular infrastructure, and it interfaces with a cellular network. The coverage of the HGW can be considered as a cell of the network, to which it is fully integrated. For such a node, the configuration parameters to be provided by the configuration server may include a radio network controller address, scrambling codes, a location area code, a routing area code, a reference macrocell identity, etc.

[0056] Of course, the present invention may apply to various other types of nodes as well.

What is claimed is:

1. A method of authorizing a first node for receipt of information from a communication network, the first node having a public key which is a function of an identifier associated with the first node and a secret key related to the public key, the method comprising, at a second node of the communication network:

authenticating the first node using an identity-based authentication algorithm based on the public key and the secret key; and

when the first node is successfully authenticated, permitting the first node to receive information from the communication network.

2. The method of claim **1**, wherein the public key is the identifier associated with the first node.

3. The method of claim **1**, wherein the public key is derived from the identifier associated with the first node.

4. The method of claim **1**, wherein authenticating the first node using an identity-based authentication algorithm comprises:

receiving information from the first node at the second node; and

confirming, at the second node, that the received information was derived using the secret key for the first node.

5. The method of claim **1**, wherein permitting the first node to receive information from the communication network comprises transmitting information from the second node to the first node.

6. The method of claim **1**, wherein permitting the first node to receive information from the communication network comprises transmitting configuration information from the second node to the first node.

7. The method of claim **1**, wherein, before the first node is authenticated by the second node, the first node has no parameters for accessing the communication network other than the public key, the secret key and at least one network address, the at least one network address comprising a network address of the second node.

8. The method of claim **1**, wherein the public key comprises a one-way function of the identifier associated with the first node.

9. The method of claim **8**, wherein the one-way function comprises a hash function.

10. The method of claim **1**, further comprising:

generating the secret key from the identifier associated with the first node; and

providing the secret key to the first node.

11. The method of claim **1**, further comprising transmitting information to the first node via the communication network.

12. The method of claim **11**, wherein transmitting information to the first node comprises transmitting encrypted information to the first node.

13. The method of claim **12**, wherein transmitting encrypted information to the first node comprises transmitting information encrypted using identity-based encryption.

14. A system for authorizing a first node for receipt of information from a communication network, the first node having a public key which is a function of an identifier associated with the first node and a secret key related to the public

key, the apparatus comprising a second node of the communication network, the second node comprising:

a communication interface; and

a processor coupled to the communication interface, the processor being configured:

to authenticate the first node using an identity-based authentication algorithm based on the public key and the secret key; and

when the first node is successfully authenticated, to permit the first node to receive information from the communication network.

15. The system of claim **14**, wherein the public key is the identifier associated with the first node.

16. The system of claim **14**, wherein the public key is derived from the identifier associated with the first node.

17. The system of claim **14**, wherein the processor is configured to authenticate the first node using an identity-based authentication algorithm by:

receiving information from the first node at the second node; and

confirming, at the second node, that the received information was derived using the secret key for the first node.

18. The system of claim **14**, wherein the processor is configured to permit the first node to receive information from the communication network by transmitting information via the communication network to the first node.

19. The system of claim **14**, wherein the processor is configured to permit the first node to receive information from the communication network by transmitting configuration information via the communication network to the first node.

20. The system of claim **14**, wherein, before the first node is authenticated by the second node, the first node has no parameters for accessing the communication network other than the public key, the secret key and at least one network address, the at least one network address comprising a network address of the second node.

21. The system of claim **14**, wherein the public key comprises a one-way function of the identifier associated with the first node.

22. The system of claim **21**, wherein the one-way function comprises a hash function.

23. The system of claim **14**, further comprising a secret generator configured:

to generate the secret key from the identifier associated with the first node; and

to provide the secret key to the first node.

24. The system of claim **14**, wherein the second node is configured to transmit information to the first node via the communication network.

25. The system of claim **24**, wherein the second node is configured to transmit information to the first node by transmitting encrypted information to the first node.

26. The system of claim **25**, wherein the second node is configured to transmit encrypted information to the first node by transmitting information encrypted using identity-based encryption.

* * * * *