(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 October 2011 (06.10.2011)

PCT

(10) International Publication Number
WO 2011/121388 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/04* (2009.01)

(21) International Application Number:
PCT/IB2010/002118

(22) International Filing Date:
30 August 2010 (30.08.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
899/CHE/2010 31 March 2010 (31.03.2010) IN

(71) Applicant *(for all designated States except US)*: **ABB RESEARCH LTD** [CH/CH]; Affolternstrasse 44, CH-8050 Zurich (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KUMAR, Ravish** [IN/IN]; c/o Ashok Kumar, Mela Road, Lohia Nagar, Sitamarhi 843302, Bihar (IN). **RAY, Apala** [IN/IN]; Santi Neer, Bosepara Bishnupur, Bankura 722122, West Bengal (IN). **KANDE, Mallikarjun** [IN/IN]; #50/1, Chandrodaya, Kadirenapalya, Indiranagar PO, Karanataka, Bangalore 560048 (IN). **NARAYANAN, Venkateswaran** [IN/IN]; 421, First Cross, Church Road, New Tippasandra, Bangalore 560075, Karnataka (IN). **KALITA, Hemanta, K.** [IN/IN]; Village Masua, P.O. Howly, Howly 781316, Assam (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: A METHOD OF SECURE MULTIPLE JOINING FOR A DEVICE TO JOIN WIRELESS SYSTEM NETWORK AND A WIRELESS DEVICE THEREOF

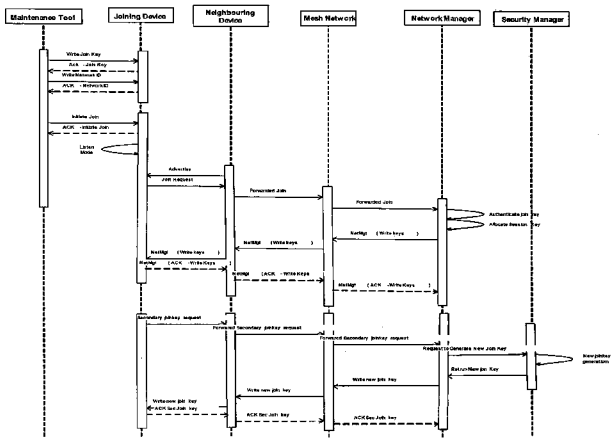

Figure 2

(57) **Abstract**: The invention relates to a method of secure multiple joining for a joining device to join a wireless system network. The method comprises the following steps. Acquiring at least one first join key; identifying the connecting device in the wireless system network; requesting the connecting device for joining the network through the connecting device identified; having an allocated session for the said joining device; acquiring the second join key from the connecting device; and replenishing the said at least one first join key with the at least one of the acquired one or more said second join key. The invention also relates to a wireless device having a first join key, capable of 'joining a wireless system network. The said wireless device is configured to receive one or more join keys from a maintenance tool or from the connecting device and replenish the first join key with the at least one of the received one or more join keys.

WO 2011/121388 A1

A METHOD OF SECURE MULTIPLE JOINING FOR A DEVICE TO JOIN WIRELESS SYSTEM NETWORK AND A WIRELESS DEVICE THEREOF

FIELD OF THE INVENTION

The present invention relates to a method of joining a wireless system network used by a device to obtain access to the network and integrate thereto in the network, and more particularly to a method of secure multiple joining for a joining device to join a wireless system network. The invention also relates to a wireless device capable of joining in a wireless system network.

BACKGROUND OF THE INVENTION

Generally, wireless system network (WSN) such as mesh networks, star networks, etc for providing higher security, enhanced performance and reduced maintenance is a network comprising wireless / field devices with sensing / transmitter / actuators and wireless communication capabilities. The wireless nodes attached to the field devices detect the event being monitored or tracked and report the information to high end devices for further control. When a new wireless node appears in the network, it is required to obtain access to the network and to become integrated into the network. To this effect, it is necessary for the new wireless node and thereby the new device to join the wireless system network. To manage wireless system network, there are one or more wireless management components such as Network manager, Security manager etc for managing the network and the security thereof.

The process of joining refers to the method or process involved therein for a device to obtain access to the network and integrate itself in to the said network. It is more apparent for a new device joining the network or for disconnected device to rejoin the network. The device which undergoes the process of joining the network hereafter is referred to as joining device. In order for a joining device to participate and become operational in the network, it is imperative to authenticate the joining device, and such authentication is performed during the joining process.

The joining process for a joining device generally pursue the sequence of obtaining the network ID, being a unique identifier for a wireless node and a Join key from a maintenance tool such as handheld device. This is followed by monitoring by the joining device to synchronize itself to the network clock and to identify the potential device already in the network, that may be used by the joining device for getting connected in the network, and the potential device mentioned above is hereafter referred as connecting device. Periodic advertise packets containing sufficient information such as time synchronization information and a unique network ID, for the joining device to synchronize to the network and communicate on the correct link, are being made by the existing devices in the network to enable the joining device to identify its connecting device already in the network, through which the joining device presents its credentials to the network manager for authentication or to demonstrate that the joining device is trustworthy. In another scenario joining device can also directly present its credentials to network manager and uses advertise packets from network manager / gate way for synchronization. The credentials include the network ID pertaining to the identity of the joining device and the Join key.

After examining the credentials of the joining device, and having met the security requirements for the said device, the network manager proceeds to integrate the joining device into the network.

In the wireless system network, due to problems relating to software, hardware or the like, the wireless node may go offline, and needs to rejoin the network when it requires to become online. It is imperative to note that during the period of the wireless node being offline, the wireless node may possibly be encountered with security threats. This is often referred to as node compromise. Node compromise usually consists of three stages namely, physically obtaining and compromising the wireless node, redeploying the compromised wireless node, and compromised wireless node launching attacks after rejoining the network.

Since, the rejoining process is in fact similar to that of the joining process involved in a joining device in joining the network and getting integrated therein, the join key can be used over and over in the network. This causes serious threat to the security of the network. Currently, the rejoining process follows the progression as described herein above making use of the join key already been assigned thereby affecting the security of the network. A method for a joining device to join a network multiple times securely is of prime relevance and consideration.

Therefore, there is a need for a method, for a joining device to securely join a network multiple times and also to evade instances of security threats in the rejoining process of a wireless node and thereupon the rejoining device.

OBJECTS OF THE INVENTION

It is an object of the present invention to provide a method which eliminates the security threat in a joining process.

It is also an object of the invention to provide a method by which the joining process is more robust and which does not compromise on security aspects of the network due to such joining process.

Another object of the invention is to provide a wireless device which is capable of secure multiple joining in a wireless system network, in accordance with the method of the invention.

SUMMARY OF THE INVENTION

The present invention is aimed at providing an improved joining and secure multiple joining process for a wireless node and therein the associated device, and a wireless device thereof.

Accordingly the present invention provides a method of secure multiple joining for a joining device to join a wireless system network. The wireless network has one or more

field device and at least one wireless management component. The wireless management component includes one or more modules such as access points, gateway, network manager and security manager. The one or more field device is connected to the said at least one wireless management component by wireless means. The said wireless system network has at least one connecting device identified from the one or more field device or from the at least one wireless management component. The method according to the invention comprises the steps of:

a) acquiring at least one first join key either alone or along with a network ID by the said joining device from a mainteneance tool or from the connecting device or from the said joining device containing the second join key replenishing the at least one first join key and being utilized as the first join key;

b) identifying the connecting device in the wireless system network, by the joining device from the one or more field device in the wireless system network based on the advertise packets of the one or more field device. The said advertise packet have sufficient information to enable the said joining device to synchronize to the network;

c) requesting the connecting device for joining the network through the connecting device identified, by the joining device, wherein the wireless management component authenticates the credentials of the joining device that includes the network ID or the join key or a combination thereof;

d) having an allocated session for the said joining device by the wireless management component. The session allocation enables the joining device to integrate and participate in the network. The session allocation is established with a session key which is same as the join key or that generated by the wireless management component;

e) acquiring the second join key from the connecting device; and

f) replenishing the said at least one first join key stored in the protected memory of the said joining device with the at least one of the acquired one or more said second join key. The said first or second join key is utilized not more than once by the said joining device in any of successful joining process.

A successful joining process besides integrating the joining device into the wireless system network also include replenishing the first join key with the second join key in the joining device. In the event of the joining device getting disconnected from the network after being integrated into the network but before receiving the second join key, the first join key may still be used to enable the joining device to undergo the successful joining process. However, the joining device upon successfully joining the wireless system network, has the first join key replenished with the second join key.

Accordingly, the present invention also provides a wireless device having a first join key. The wireless device is capable of secure multiple joining in a wireless system network. The said wireless device is configured to receive a second join key from a hand held device or from the connecting device and replenish the first join key with the atleast one of the received one or more second join key. The wireless device is attachable to or integral part of sensing or transmitting equipment in a process plant.

BRIEF DESCRIPTION OF THE DRAWINGS

With reference to the accompanying drawings in which:

Figure 1 depicts the sequence for joining process according to current practice.

Figure 2 depicts the sequence for secure joining process according to an exemplary embodiment of the invention.

Figure 3 shows the flow chart of the steps involved in secure multiple joining process in accordance with the exemplary embodiment of the invention depicted in Figure 2.

Figure 4 illustrates a wireless system network.

DETAILED DESCRIPTION

From Figure 1, it can be seen that in the current practice, the maintenance tool such as handheld device writes the join key into the joining device wherein the join key is essential for a joining device to join the network. The joining device acknowledges to the maintenance tool the receipt of the join key. Thereafter, the maintenance tool writes the corresponding network ID into the joining device and the same is being acknowledged by the joining device. The network ID is used in identifying the network to which the joining device is to join. Then the joining of the device is initiated by the joining device or by maintenance tool and the same is being acknowledged by the joining device to the maintenance tool.

At this point, the joining device is in a listening mode to synchronize itself to the network clock and to identify the connecting device already in the network and receive advertise packets from neighbour devices. In this mode the joining device identifies its neighbours and after such identification of one or more neighbouring devices, the joining device selects one of them to join through into the network. The request for joining is placed by the joining device through the selected neighbouring device and the join request is forwarded to the network manager through the wireless system network.

The network manger authenticates the credentials of the joining device and on successful authentication, the network manager allocates a session key and the allocated session key is written into the joining device. The joining device acknowledges to the network manager the receipt of such session key which has been allocated by the network manager. The session key establishes the session allocated for the joining device enabling it to participate and integrate into the network. This way, the joining process for a device is being carried out.

When the device which had already joined the network goes out of the network or when it gets disconnected, the network manager waits for a predetermined time period and on elapse of such time period the network manager deletes the session key previously allocated for the said device. In the circumstances, the device which had gone out of the network is required to follow the entire joining process as described herein above in order

to rejoin and integrate itself into the network. It is hereby understood that the process of rejoining is similar to that followed for joining process. It is to be noted that one join key used by a joining device can be reused or reutilized again in the network during subsequent joining / rejoining process. Hence, there is a high possibility of breach of security with the wireless node getting compromised by security threats.

The present invention eliminates such security threats and renders the joining / rejoining process for a device more robust.

Considering the invention as described herein above in the summary, the present invention is explained further with reference to a non exhaustive exemplary embodiment of the invention purporting to Figures 2 to 4. However, the method as explained with reference to an exemplary embodiment includes the steps of: acquiring the first join key; identifying the connecting device in the mesh wireless system network; requesting the connecting device for joining the network through the connecting device identified; having a session allocated for the said joining device; acquiring the second join key from the connecting device; and replenishing the said first join key with the acquired said second join key.

The method of joining referred herein in the context of the invention includes the method of secure multiple joining for a joining device to join the wireless system network for the first time and / or for subsequent time(s) which may be multiple or for rejoining the network when the said joining device goes out of the network or when disconnected from the network. The term secure multiple joining referenced herein in the description includes first time joining.

Figures 2, 3 and 4 show the sequence for joining process, the flow chart of the steps involved in joining process and the system, having relevance to the present invention.

In consideration with the wireless system network (400) capable of performing the method of the invention or that purported by the prior art or both, at step (301), in

accordance with the method of the invention, the maintenance tool writes the join key into the joining device. The join key here being the first join key, and the hand held device being wire connected to the joining device or being a wireless device having a short range wireless communication which could safely and securely load the said first join key into the joining device without any intrusion or interference from the other elements / components in the network.

At step (302) , the joining process is initiated and the joining device is in listening mode where it is monitoring to synchronize itself to the network clock and identify a connecting device in the network through which it can place its credentials to the network manager (401) for authentication and thereupon for integration into the network. The connecting device mentioned herein can be a field device (403) already integrated in the network and more likely from one of the neighbouring devices or one from a wireless management component as referred herein before in the description, which include one or more modules such as access points (404), gateway (405), network manager (401) and security manager (402). The wireless management component is accountable for the functioning of the network.

During the listening mode the joining device receives advertise packets containing sufficient information for the joining device to synchronize to the network and communicate on the correct link, from the one or more neighbouring devices to enable the joining device to identify its connecting device, one from the field devices (403) already in the network, through which the joining device presents its credentials to the network manager (401) for authentication or to demonstrate that the joining device is trustworthy and this has been represented as step (303). It is to be noted that the advertise packets can also be received from the access points (404).

After successful identification of the connecting device for a joining device to join the network, the joining device sends a request for joining to the network manager (401) through the neighbouring device identified as its connecting device for joining and through the network. This is depicted in step (304). The wireless system network referred

herein includes the field devices (403) which are in engagement with each other, access points (404) and the gateway (405). On successful authentication of the credentials of the joining device, the network manager (401) allocates a session key for the joining device and the same is written into the joining device and can be referred to step (305). The session key could be the same as the join key or the one generated by the wireless management component. The session key establishes a session for the said joining device to enable to integrate into the network and participate in the network and become operational thereby.

The invention besides utilizing a first join key initially used by a joining device for joining the wireless system network, also employs a second join key. The joining device after successful integration into the network and having joined the network, makes a request to the network manager (402) through the connecting device for generating a new join key by the security manager (402) as inferred from step (306). At step (307), the new join key is generated by a key generation module of the security manager (402) of the wireless management component. The said module besides generating the join key manages the generated join key(s) in the manner already known. The new join key is generated on the basis of one or more of device MAC address, join time, join key expiration period, key index, temperature, CPU speed, network ID as seed, or any such parameters. The generation of a join key highly randomized by means of parametric based join key generation which would generate dissimilar join keys each time it is generated. At step (308), the new join key so generated by the wireless management component and been communicated to, and stored in the joining device, conforms to the second join key for the said joining device. Here, it is to be noted that one or more new join keys may be generated by the wireless management component and the same be acquired and stored in the said joining device. The exemplary embodiment is explained herein with reference to one second join key. However, it is to be construed that the second join key may be from the at least one of the received one or more join keys.

Likewise, the exemplary embodiment describes the use of one join key for one joining process. However, the method of the invention can easily be extended for use of multiple

join keys for one joining process. In a scenario where the system uses multiple join key for a joining process, the first join key and the second join key as described in the invention are to be construed as containing multiple first join keys and multiple second join keys respectively for corresponding joining process. It is to be noted that multiple join keys i.e, first join key(s) and secondary join key(s) can be employed in a joining process as referred herein above and they may be fragmented (distributed in parts) and distributed in the wireless sensor network system by the wireless management component synchronized with one of the technique described in the invention such as secondary key identification number, common time stamp, number of joins. The join key when distributed in parts, the joining device is capable to receive the distributed part of the key and assemble them to form the join key to join the network. Any well known technique maybe used for fragmentation and assembly of keys.

In this context, join key initially used by the joining device at its first instance in any joining process becomes the first join key and that later acquired from the wireless management component becomes the second join key. Here, the second join key is required to be used by the said joining device in the event of rejoining the network, which follows the same progression of the joining process as mentioned earlier herein above. The second join key replenishes the first join key stored in the protected memory of the joining device. The term "replenish" is used herein in the description in the context to indicate that, when the second join key is used for joining the network subsequently and the first join key will be abandoned / not used for subsequent joining. As one may note multiple embodiments may be included illustrating a particular scheme of implementation and this includes an embodiment for having a separate storage of the second join key in the protected memory along with the first join key. Upon utilization of the second join key as the first join key for the joining / rejoining process, as the previous join key identified as first join key can no more be used in the joining process, it is required that the joining device make a further request to the wireless management component for a new join key. Now, the new join key as generated by the wireless management component becomes the second join key replacing the previous second join key which has been used as the first join key for joining / rejoining the network during

immediate previous instance. In this manner, the second join keys are generated and it replenishes the previously generated second join keys. If the joining device goes out of the network after integrating into the network but before receiving the second join or in the absence of availability of second join key or in case of joining device which does not support the second join key, the first join key can still be used to have a successful joining process. Here, the successful joining process is to be construed to include receiving and replenishing the first join key of the joining device besides integrating into the network.

The method of the invention as described herein above is available in a device such as field devices eg. sensors, transmitters or any other sensing and monitoring devices, either as integral part or as an attachment for wireless activities or simply activities related to secure joining.

Rejoining process could be also through pre-stored join keys. The pre-stored join keys may include the one or more join keys already stored in the joining device after successful joining process. In the event of the joining device leaving the wireless system network, the said joining device joins the network using the pre-stored join key in synchronization with the wireless management component. The synchronization between wireless management component and joining device is accomplished using a common counter based on number of times joining device had joined or left the wireless system network. The number of pre-stored join keys that has to be stored in joining device and / or wireless management component can be configured and will be refreshed or stored again with new values each time the joining device leave and rejoin the wireless system netwrok.

The above explained process eliminates the threat of security breach when a wireless node and its corresponding device goes out of network or gets disconnected, since a join key is not utilized for the second time in a successful joining process. Therefore, the wireless node does not get compromised.

If any device attempts to intrude into the network by placing a wrong join key, such attempt for intrusion is detected and suitable alarm may be raised accordingly. Also, any attempt to use an invalid / wrong join key more than a predetermined number of times (ideally two times but more rigidly once) renders the MAC address pertaining to that particular wireless node from which such attempts are made, to be blocked and alarm may be raised, so as to prevent as well as detect any intrusion.

Further, the wireless management component monitors the expiration of the join key and its renewal, and the requests made for a new join key. This could become part of the periodic surveillance over the network or may be done independent of such surveillance.

It is to be noted that any possible variations and modifications other than that been described in the specification, but inferred there from in the context of the invention, be construed to be well within the scope of the invention though not explicitly referred.

I/WE CLAIM:

1. A method of secure multiple joining for a joining device to join a wireless system network having one or more field device and at least one wireless management component including one or more modules such as access points, gateway, network manager and security manager, the said one or more field device is connected to the said at least one wireless management component by wireless means, the said wireless system network has at least one connecting device identified from the one or more field device or from the at least one wireless management component, the said method comprising the steps of:

acquiring at least one first join key;

identifying the connecting device in the wireless system network;

requesting the connecting device for joining the network through the connecting device identified;

having an allocated session for the said joining device;

acquiring one or more second join key from the connecting device; and

replenishing the said at least one first join key with at least one of the acquired one or more said second join key.

2. The method as claimed in claim 1 comprising the step of acquiring the join key either alone or along with a network ID by the said joining device from maintenance tool or from the connecting device or from the said joining device containing the at least one of the one or more second join key replenishing the said at least one first join key and utilizing as the first join key.

3. The method as claimed in claim 1 comprising the step of identifying the connecting device by the joining device from the one or more field device in the wireless system network based on the advertise packets of the one or more field device, the said advertise packet have sufficient information to enable the said joining device to synchronize to the network.

4. The method as claimed in claim 1 comprising the step of requesting the connecting device identified, for joining the network by the joining device, wherein the wireless management component authenticates the credentials of the joining device that includes the network ID or the join key or a combination thereof.

5. The method as claimed in claim 1 comprising the step of having an allocated session for the said joining device by the wireless management component, wherein the session allocation enables the joining device to integrate and participate in the network.

6. The method as claimed in claim 5, wherein the said allocated session is established with a session key which is same as the join key or that generated by the wireless management component.

7. The method as claimed in claim 1 comprising the step of replenishing the said at least one first join key stored in the protected memory of the said joining device with the at least one of the acquired one or more said second join key.

8. The method as claimed in claim 1, wherein the said first or second join key is utilized not more than once by the said joining device in any of successful joining process.

9. A wireless device having a first join key, capable of joining a wireless system network, the said wireless device is configured to receive one or more join keys from a maintenance tool or from the connecting device and replenish the first join key with the at least one of the received one or more join key.

10. The wireless device as claimed in claim 9, wherein the said wireless device is attachable to or integral part of sensing or transmitting equipment in a process plant.

11. The wireless device as claimed in claim 9, wherein the said wireless device is capable of receiving at least one join key distributed in parts and of assembling the received join key in parts to form the join key to join the wireless system network.

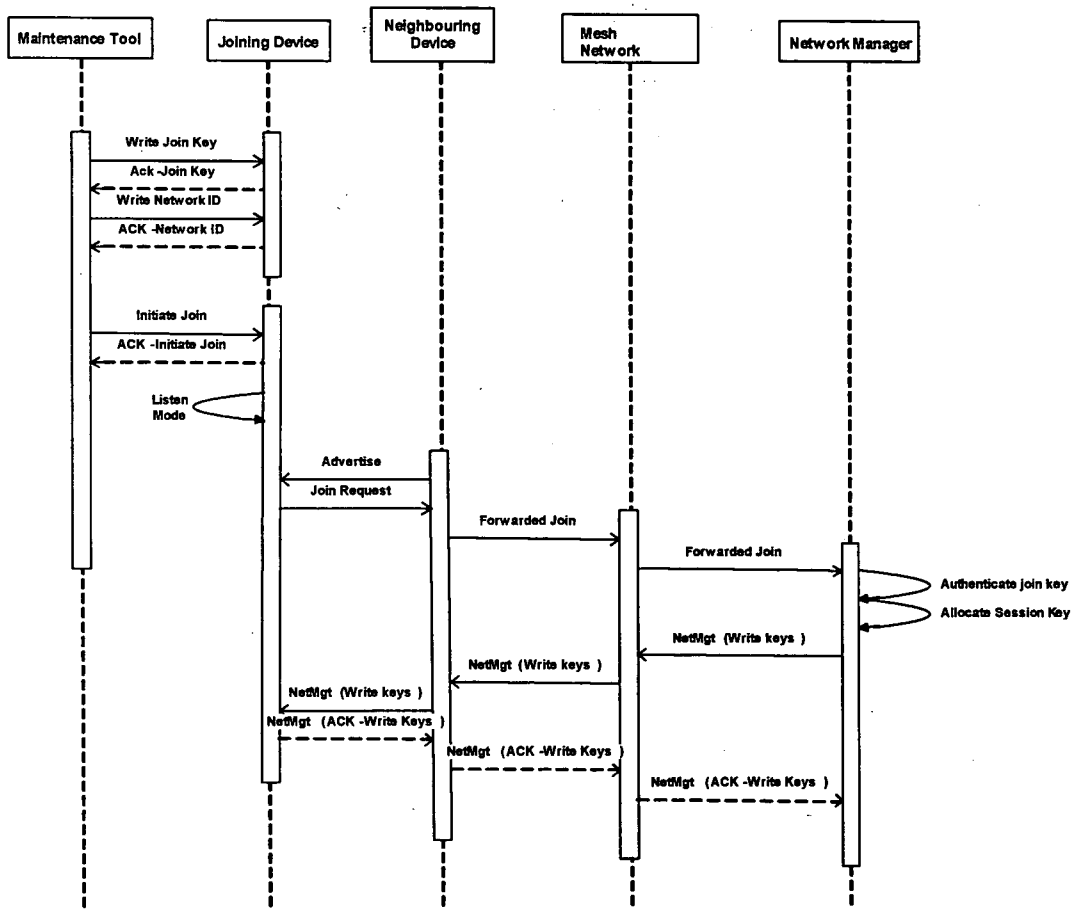
Maintenance Tool
Joining Device
Neighbouring Device
Mesh Network
Network Manager
Write Join Key
Ack -Join Key
Write Network ID
ACK -Network ID
Initiate Join
ACK -Initiate Join
Listen Mode
Advertise
Join Request
Forwarded Join
Forwarded Join
Authenticate join key
Allocate Session Key
NetMgt (Write keys)
NetMgt (Write keys)
NetMgt (Write keys)
NetMgt (ACK -Write Keys)
NetMgt (ACK -Write Keys)
NetMgt (ACK -Write Keys)

Figure 1

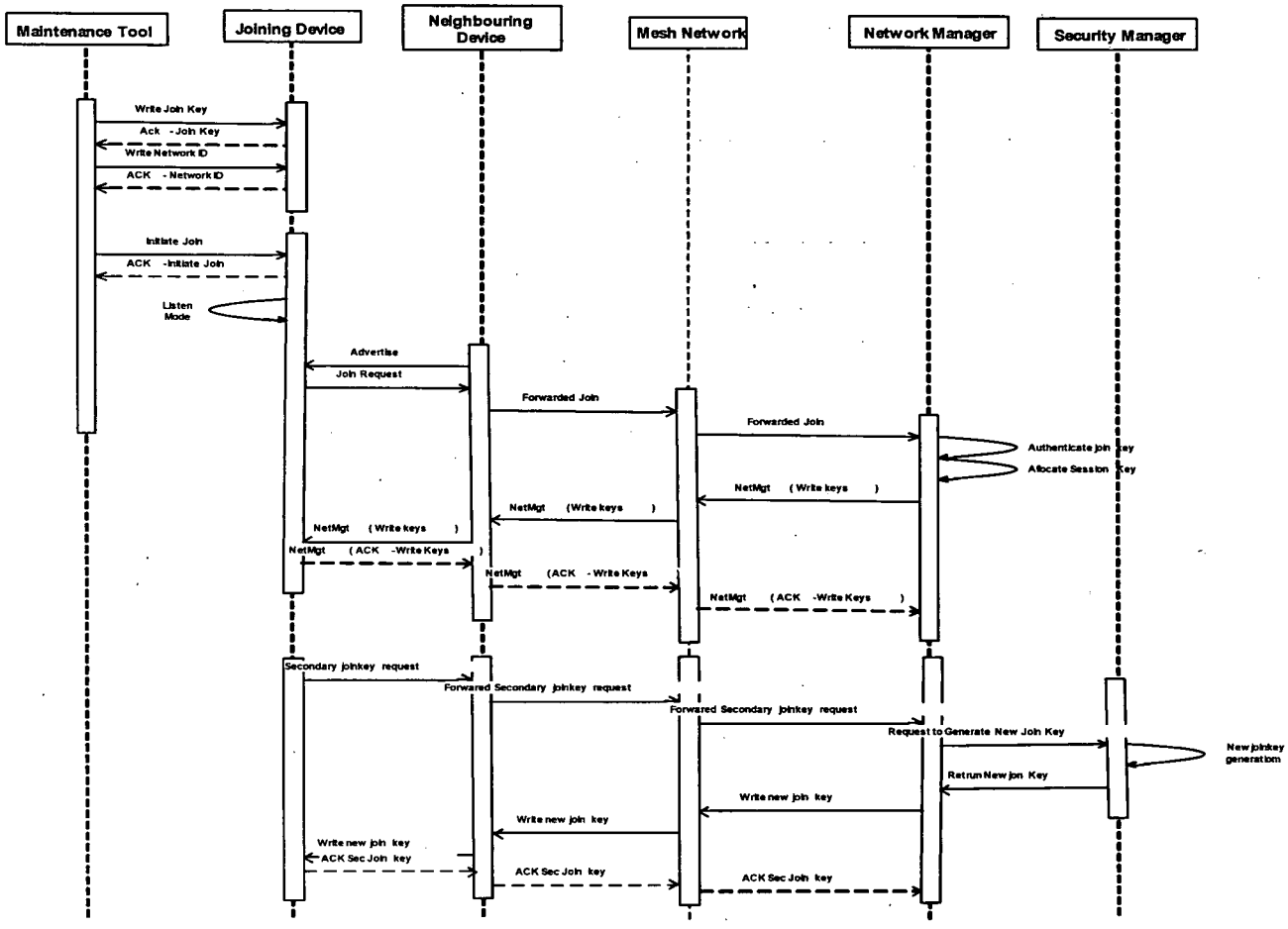
Maintenance Tool
Joining Device
Neighbouring Device
Mesh Network
Network Manager
Security Manager
Write Join Key
Ack - Join Key
Write Network ID
ACK - Network ID
Initiate Join
ACK -Initiate Join
Listen Mode
Advertise
Join Request
Forwarded Join
Forwarded Join
Authenticate join key
Allocate Session Key
NetMgt (Write keys)
NetMgt (Write keys)
NetMgt (Write keys)
NetMgt (ACK -Write Keys)
NetMgt (ACK - Write Keys
NetMgt (ACK -Write Keys)
Secondary joinkey request
Forwared Secondary joinkey request
Forwared Secondary joinkey request
Request to Generate New Join Key
New joinkey generation
Retrun New join Key
Write new join key
Write new join key
Write new join key
ACK Sec Join key
ACK Sec Join key
ACK Sec Join key

Figure 2

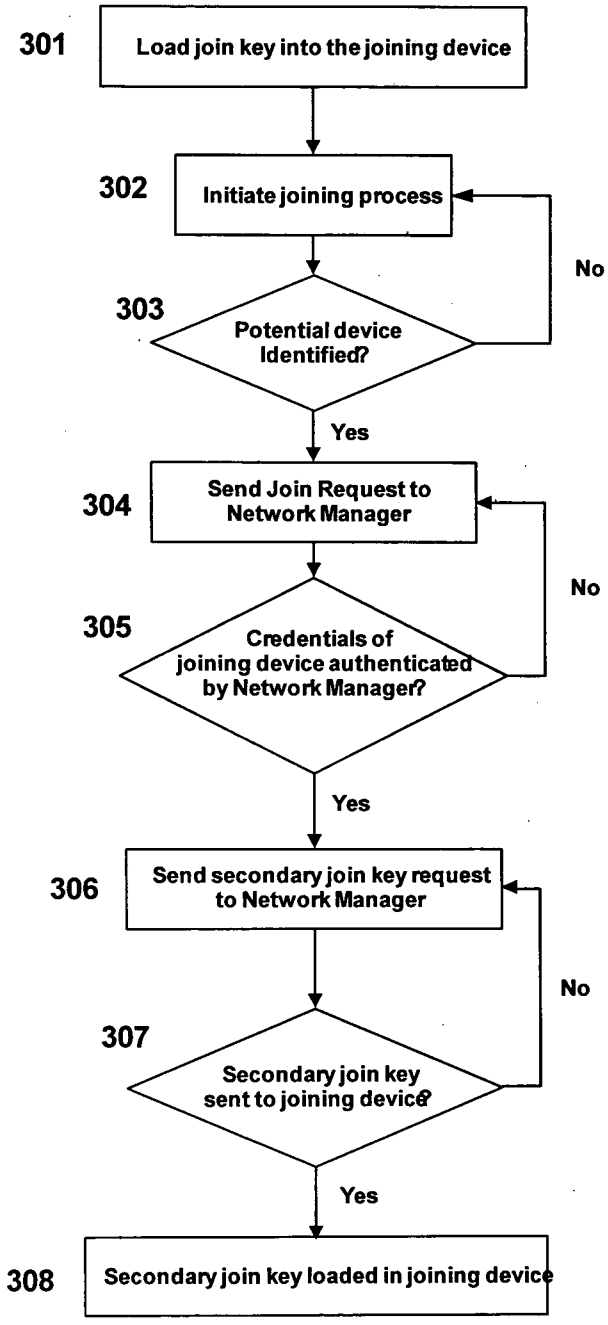
301
Load join key into the joining device
302
Initiate joining process
No
303
Potential device Identified?
Yes
304
Send Join Request to Network Manager
No
305
Credentials of joining device authenticated by Network Manager?
Yes
306
Send secondary join key request to Network Manager
No
307
Secondary join key sent to joining device?
Yes
308
Secondary join key loaded in joining device

Figure 3

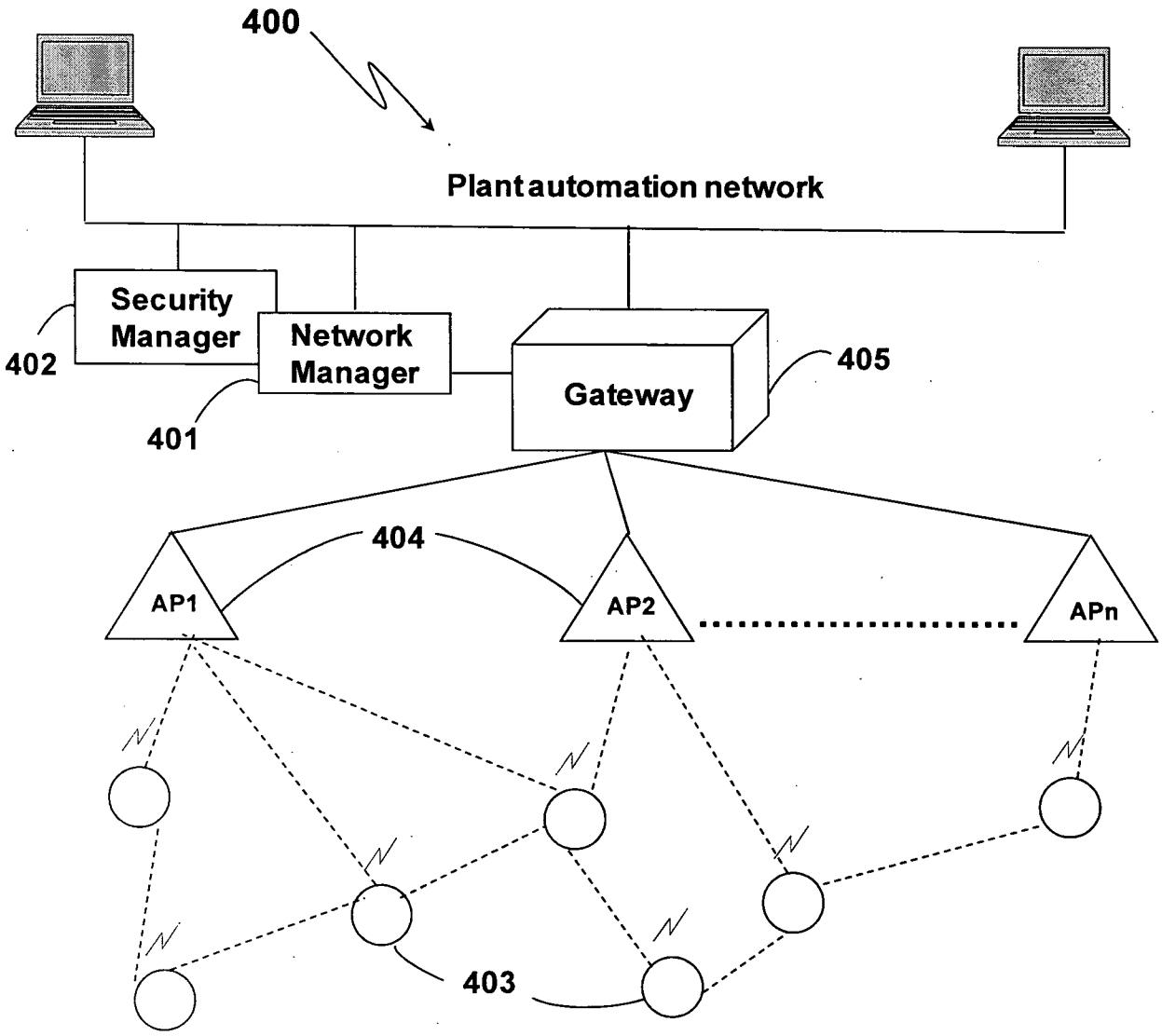
400
Plant automation network
Security Manager
Network Manager
Gateway
402
401
405
404
AP1
AP2
APn
403

Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/002118

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JUN-CHEOL JEON ET AL: "Non-group Cellular Automata Based One Time Password Authentication Scheme in Wireless Networks" In: "SECURE MOBILE AD-HOC NETWORKS AND SENSORS, LECTURE NOTES IN COMPUTER SCIENCE" 1 January 2006 (2006-01-01), SPRINGER , BERLIN, DE, , XP019037297 ISBN: 978-3-540-36646-1 vol. 4074, pages 110-116, abstract Section 1 ----- -/--	1-11

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 January 2011	22/02/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bertolissi, Edy

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/002118

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Chapter 10: Identification and Entity Authentication ED" In: Menezes A J; Van Oorschot P C; Vanstone S A: "HANDBOOK OF APPLIED CRYPTOGRAPHY" [Online] 1 October 1996 (1996-10-01), CRC PRESS, SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS , BOCA RATON, FL, US , XP001525010 ISBN: 978-0-8493-8523-0pages 385-424, Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ > Section 10.2.5 -----	1-11
A	FIRDOUS KAUSAR, ASHRAF MASOOD AND SAJID HUSSAIN: "An Authenticated Key Management Scheme for Hierarchical Wireless Sensor Networks"[Online] 2008, pages 1-15, XP002618290 ADVANCES IN COMMUNICATION SYSTEMS AND ELECTRICAL ENGINEERING - LECTURE NOTES IN ELECTRICAL ENGINEERING Retrieved from the Internet: URL:http://cs.acadiau.ca/~shussain/wsn/publications/08-csee.pdf> [retrieved on 2011-01-25] abstract Sections 1, 2 and 3 -----	1-11