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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2012 (01.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/148257 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04K 1/00* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/MY2012/000090

(22) International Filing Date:
26 April 2012 (26.04.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2011001845 26 April 2011 (26.04.2011) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **USMAN, Sarwar** [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **GOPINATH, Rao, Sinniah** [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **REZA, Khoshdelniat** [IR/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **ZELDI, Suryady** [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(74) Agent: **MANIAM, Mahalingam**; IP Rights (m)sdn Bhd, No. 7-M, Biz Avenue, Neo Cyber, Lingkaran Cyber Point Barat, 63000 Cyberjaya, Selangor Darul Ehsan (MY).

(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, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, RS, 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 the identity of the inventor (Rule 4.17(i))*

[Continued on next page]

(54) Title: METHOD FOR USE IN MULTI HOP WIRELESS SENSOR NETWORK

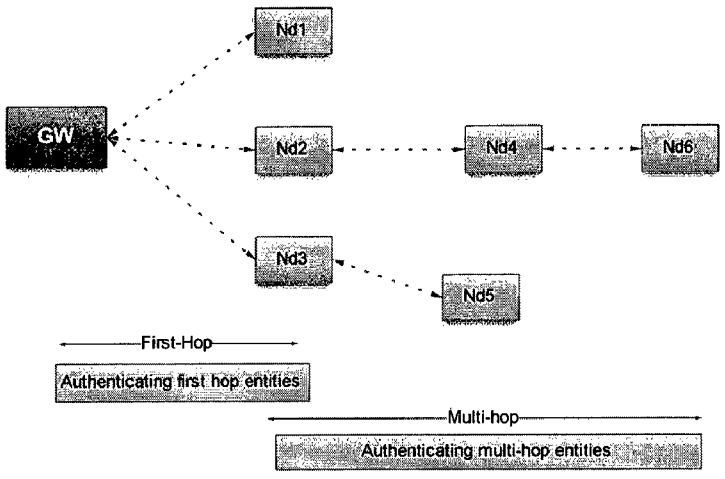

FIG 1

(57) Abstract: The present invention relates to a method for use in a wireless sensor network comprising at least one gateway and at least two nodes; said method comprising the steps of: performing a bi-directional authentication between nodes and between node and gateway; defining and selecting an authentication header between available nodes, wherein said header contains information related to authentication, level of security for authentication and authentication messages; providing authentication information with a predetermined amount of times on validation failure; and forbidding an unknown entity from entering the network in the event that the validation failure exceeds the predetermined amount of time.

WO 2012/148257 A1

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD FOR USE IN MULTI HOP WIRELESS SENSOR NETWORK

FIELD OF INVENTION

The preferred embodiments of the present invention directs to a method for use in a wireless sensor network, and more particularly a method for use in a multi hop wireless sensor network.

BACKGROUND

The need to improve the operative efficiency in wireless sensor networks has been progressively emerging and thus placed as a significant target among researchers and innovators of the relevant art when developing advanced wireless sensor network paradigm. Further, the rapid growth in global accessibility results to incessantly seek solutions in creating methods or systems which are robust and reliable. The main challenges include providing resilient, cost efficient and secured connections for future generation networks.

In most instances however, wireless networks are vulnerable in terms of security, whereby they are prone to malicious attacks by unknown or uncertified entities. Abusers may deploy various types of assaults to disrupt the purpose of wireless networks, such as injecting into the data packets or changing the routes of packet destinations and jamming the signal. Such disruption may jeopardize an important data transmission between a sender and recipient. One of the common steps involved when infiltrating networks is becoming part of the network or in other words undetectably joining the network. Moreover, nowadays, in order to ensure seamless and reliable connection, wireless networking is commonly associated with

multi-hop networking and mesh networking, in which for such network, information is conveyed or routed from a source to a destination using two or more networks. Disruptions due to malicious attacks therefore are expected to increase.

In order to alleviate the shortcoming as described above, more networks deploy authentication mechanisms, whereby nodes is subjected to at least one form of authentication process prior to joining the sensor network. This current ultimatum maybe be expedient at a certain level however other problems would surface including such as complicated protocols for authentication of wireless sensor network entities, failure to accommodate issues relating to malicious gateways or mobile based full function device (FFD) and using single level of security for all types of use-cases which prove to be ineffective purely because security applicability varies subject to different types of applications.

An exemplary of a related prior art as one of the available solutions to improve wireless network security is as disclosed in United States Patent Application US 20090103731 – *Authentication of 6LoWPAN Nodes Using EAP-GPSK.* The invention relates to a method of authentication which promotes exchanging extensible authentication protocol messages for authentication by sending a plurality of packets formatted in the form of the suitable wireless network protocol. Nonetheless, this prior art does not disclose any information in relation to providing bi-directional authentication of each entity which may be involved using a distributed mechanism and the messaging protocol disclosed in this prior art seems to be rather complex.

Recognizing the aforementioned shortcomings associated to the prior art and existing systems, the present invention has been accomplished to significantly improve the conventional methods and systems.

It is therefore another object of the present invention to provide a method for use in multi-hop wireless sensor network, said method and system provides expediency in providing secured connection within said wireless sensor network.

It is further object of the present invention to provide a method for use in multi-hop wireless sensor network, said method and system is highly reliable and economical.

It is another object of the present invention to provide a method for use in multi-hop wireless sensor network, said method and system aids to protect the network from hazardous intrusions.

Still other objects of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein embodiments of the invention are described by way of illustration. As will be realized, the invention is capable of other and different embodiments and its several details are capable of modifications in various respects, all without departing from the spirit and the scope of the present invention.

SUMMARY OF INVENTION

The present invention discloses a method for use in a wireless sensor network comprising at least one gateway and at least two nodes ; said method comprising the steps of: performing a

bi-directional authentication between nodes and between node and gateway; defining and selecting an authentication header between available nodes, wherein said header contains information related to authentication, level of security for authentication and authentication messages; providing authentication information with a predetermined amount of times on validation failure; and forbidding an unknown entity from entering the network in the event that the validation failure exceeds the predetermined amount of time.

BRIEF DESCRIPTION OF THE FIGURES

The invention will be more understood by reference to the description below taken in conjunction with the accompanying drawings herein:

FIG 1 provides an overview of authentication mechanism in multi-hop environment;

FIG 2 provides an overview of authentication protocol phases;

FIG 3 provides an overview of authentication header format in accordance with the present invention;

FIG 4 provides an overview of a different level of security in a single use-case;

FIG 5 provides a sequence flow of messages between a node and gateway in accordance with the present invention;

FIG 6 provides a flow chart of node authentication with the gateway;

FIG 7 provides a sequence flow of messages between node, node head and a gateway;

FIG 8 provides a flow chart of node authentication in multi-hop environment; and

FIG 9 provides an example of application of the present invention.

DETAILED DESCRIPTION

In addition to the drawings, further understanding of the object, construction, characteristics and functions of the invention, a detailed description with reference to the embodiments is given in the following.

In the following description, reference is made to the accompanying drawings where, by way of illustration, specific embodiments of the invention are shown. It is to be understood that other embodiments may be used as structural and other changes may be made without departing from the scope of the present invention. Also, the various embodiments and aspects from each of the various embodiments may be used in any suitable combinations. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

The present invention generally relates to an authentication mechanism which aids to authorize all the entities or nodes prior to joining a network. In one embodiment of the present invention, validation of nodes is performed in single and multi-hop network topologies.

The method of the present invention generally comprises of three main stages, these are: performing a bi-directional authentication processes, whereby authentications are carried out between gateway and nodes, as well as node and node; defining a compressed authentication header, said header contains information related to facilitating authentication, level of security required and authentication message type; and providing authentication information

with a predetermined countable limit on validation failure prior to forbidding the entry of a malicious entity. Each of the stages will be described in detail hereinbelow.

FIG 1 illustrates a high level overview of communication and authentication in multi-hop environment. In this environment, a gateway GW (10) is communicating with several nodes (11, 12, 13, 14, 15, 16) in the sensor network. Typically, nodes would perform gateway discovery so to search for suitable gateways in order to join a network. A node would later on perform an authentication procedure upon selected the gateway and said gateway would proceed with the same procedure for affirmation.

From the above, in FIG 1, GW (10) authenticates Nd1, Nd2 and Nd3 at single-hop level. Nd1 represents a normal node whereas Nd2 and Nd3 are qualified node-head at first hop level to the gateway. It should be mentioned that a node-head is a node entity which has enough resources to take responsibility of authenticating nodes at multi-hop level for the gateway. Nd4 is a second hop level node-head authenticating Nd6 and relaying it to the gateway through Nd2. Nd5 is a normal node authenticated by the Nd3.

In a further aspect of authentication, there are two set of keys used for authentication protocol by the nodes; these keys are specifically for gateway authentication and the node-head authentication. According to the present invention, authentication key for gateway and node-head are pre-deployed to the sensor network.

As briefly described above, the authentication protocol is divided into two phases which is illustrated as Phase 1 and Phase 2 as seen in FIG 2. In the Phase 1 (S100), gateway is configured to authenticate the first hop level nodes and assigns node-head status to those

which are qualified and have enough resources to be relay-authentication nodes. In Phase 2 (S200) nodes with the node-head capabilities authenticate multi-hop level nodes. During this process, node-head also identifies and assign responsibility of node-head to those nodes with enough resources.

In the preferred embodiment of the present invention, the identification of a header is crucial as it is assigned to inform important information about the authentication process. The extension header used for the present invention is known as compact authentication header (cAH) which consists of one byte. An exemplary of such header (40) is illustrated in FIG 3. The header is part of the 6LoWPAN payload and as mentioned, informs about crucial information for authentication process. A packet will be considered as an authentication packet, if the authentication header's first two bits are 1 and 0. The third and fourth bits of authentication header are use for security level fields which is considered as vital information for providing variable strength of authentication information.

Preferably, in terms of informing the level of security required, there are three types of information highlighted by security level fields. Basic level, intermediate level and advance level security which is implemented using two bits as 0 1, 1 0 and 1 1 respectively. The next four bits are used for informing about the authentication message type. This is highlighted in TABLE 1 below. The authentication messages are used by the authentication protocol for validating different entities in a sequential process which will be described herein.

TABLE 1

Authentication Message Type

Message Type	**Value**
REQ_ST	0 0 0 1
RESP_AUTH_P	0 0 1 0
RESP_AUTH_C	0 0 1 1
RESP_AUTH_SUCCESS	0 1 0 0
REQ_AUTH_RESPONSIBILITY	0 1 0 1
REQ_AUTH_RESPONSIBILITY_SUCCESS	0 1 1 0
RESP_RESPONSIBILITY_SUCCESS	0 1 1 1
RESP_AUTH_NH	1 0 0 0
RESP_AUTH_C_LN	1 0 0 1
RESP_AUTH_C_SUCCESS_LN	1 0 1 0
REQ_AUTH_P	1 0 1 1
REQ_AUTH_C	1 1 0 0
Reserve for future use	1 1 0 1 to 1 1 1 1

According to the present invention, authentication protocol also includes level of security which can be use for different use-cases. The purpose of security level is to allow different configurable sizes of authentication information for providing variable level of protection. There are three categories of authentication security levels illustrated for authentication protocol of the present invention, these are; basic level with a payload size of 8 bytes with simpler encryption, intermediate level with a payload size of 16 bytes with decent level of encryption system and advance level with a payload size of 32 bytes with complex encryption system.

It is preferred that higher the size will provide more secure authentication information but with the impact on processing and power resources. Basic security level will take lesser resources but will provide simpler authentication information. The level of security may be required for encryption system on authentication information depending on the category of

security; for instance, basic level security may use XOR based encryption whereas advance level may acquire complex encryption system like AES.

TABLE 2 illustrates an example of security levels with the possible encryption systems. The level of security is configured in pre-deployed phase of sensor network depending on the use-case. When any entity in the sensor network environment receives authentication information, it decrypts the information based on defined encryption type in the authentication header and validates it.

FIG 4 illustrates a scenario whereby wireless sensor network clusters exist with different levels of security within a single deployment.

TABLE 2

Examples in Security Levels

Security Levels	**Examples**
Basic	8 bytes authentication information with XOR based encryption
Intermediate	16 bytes authentication information with Blowfish
Advance	32 bytes authentication information with AES (32 to 128 bit)

It should be noted that based on one embodiment of the present invention, authentication information varies with different levels of security. It may contain existing methods for authentication information such as random number generation, hash tables and semantics.

FIG 5 and FIG 6 illustrate the authentication process in sequence diagram format in accordance with the preferred embodiment of the present invention. As seen in FIG 5

authentication procedure is instigated by the node by sending REQ_ST message to available gateway or node-head.

Still referring to FIG 5 and FIG 6, the node will only send a request (A100) to most suitable gateway or node-head which is within its range. REQ_ST message is customized accordingly to convey or contain private information which can only be understood by the authorize network entities. According to pre-configured security level, said node will use authentication information (A200) which is included in the REQ_ST message. When the gateway receives said REQ_ST message, it acknowledges such request (A300) and that there is a node requesting for authentication initiation procedure. The gateway will proceed to prepare and send RESP_AUTH_P message and includes authentication information for the node to validate. The authentication information is an encrypted data that need to be verified by the receiving entity and it will be stored based on security level with variable size according to strength required for the use-case.

Subsequently, node receives and validates the RESP_AUTH_P message from the gateway based on authentication information provided (A400). In the case of failure in the validation procedure, node may request the gateway by sending REQ_AUTH_P for multiple times (A500) before forbidding it. In the case of success, node will register the gateway and send back RESP_AUTH_C message. This message includes success of registering the gateway as well as node's authentication information. The gateway validates (A600) the node by checking authentication information provided in the message. In case of authentication failure, gateway requests the node by sending REQ_AUTH_C message. If the validation fails for multiple times, the gateway will forbid (A700) the node to join the network and record

this information. If the authentication information provided by the node successfully validated, node will be accordingly registered with the gateway for future operations.

In the following stage, upon completion of the node validation, gateway inquires (A800) from the node if it can take responsibility as a node-head based on its available resources. This message is conveyed to the node using REQ_AUTH_RESPONSIBILITY message. Node inspects its resources (A900) such as, but not limiting to, battery level, memory resources and RSSI value; and accordingly response back to the gateway. If the node has enough resources it will send a response back with RESP_AUTH_RESPONSIBILITY_SUCCESS message. Alternately if the node does not have enough resources, it will send back RESP_AUTH_RESPONSIBILITY_FAIL message which informs (A900a) the gateway to consider the node as a normal node. In the event that the gateway receives the message RESP_AUTH_RESPONSIBILITY_SUCCESS, gateway will register (A900b) the node as a node-head for authenticating other nodes at multi-hop level from the gateway.

FIG 7 and FIG 8 show sequential flow of multi-hop authentication procedure between node-head, node-n and the gateway. Referring to FIG 7 and FIG 8, node-n initiates the authentication procedure (T100) by sending REQ_ST message to the node 1 (node-head). The node-head sends RESP_AUTH_NH message (T200) by including authentication information to node-n. When node-n receives the message, it will understand that it is communicating and authenticating with a node-head rather than directly with the gateway. Hence on receiving the message, node-n uses node-head key to authenticate the node-head (T300). On successful validation, node-n notifies authentication information (T400) to the node-head by sending RESP_AUTH_C message. In the event of validation failure, the node

attempts n (predetermined amount) times (T500) to request the node-head for providing proper authentication information by sending REQ_AUTH_C message. If no proper information is provided, node will terminate communications with the current node-head and will further search for more node-head or the gateway. When node-head receives RESP_AUTH_C message, it authenticates the information provided by the node-n and in case of successful validation of authentication information it registers node-n (T600) as a valid node and sends RESP_AUTH_C_LN message to the gateway for registration. Gateway on receiving information (T700) about node-n, understands that node-n can be accessed through node-1 (node-head). Gateway saves this information for future communication and send acknowledgement to node1. If the validation of node-n fails (T800), node-head will request back the node-n by sending REQ_AUTH_C message n times prior to forbidding it. In accordance with the present invention, a similar procedure will be performed for determination of node-n to work as a node-head by node1(node-head).

Furthermore in case of node (node-head) failure or topology change, a node may require to access the network using other accessible node-head or gateway within its range. The joining to a new node-head or gateway will also require re-authentication.

An exemplary of an application having implemented the method and system of the present invention is shown in FIG 9. In this exemplary, there is provided a wireless sensor network in precision agriculture domain, whereby the authentication method is based on the present invention.

Now referring in FIG 9, there is provided a gateway (GW), and a plurality of nodes, namely, Node 1(Node-head), Node 2, Node 3 (Node-head), Node 4 in a green house environment.

Due to the precision agriculture use-case requirement, basic security level (8 bytes authentication information using hash values with simple encryption like XOR) will be feasible to use as the stake of security vulnerability is less. Node 1 will initialize the authentication procedure before joining the network by requesting suitable available gateway to provide authentication information. After authentication and taking responsibility of node-head, Node 1 will authenticate Node 2 and Node 3 at hop-level 2 from the gateway. Node 2 will be treated as a normal node due to lesser resources respond whereas Node 3 will take the responsibility of Node-head at hop-level 2. Node 4 will analyze the suitable gateway or node-head within its range and will choose node 3 for authenticating point to join the network at hop level 3. All the node-heads will also inform the gateway about the authenticated nodes for the future communications.

The present invention may be modified in light of the above teachings. It is therefore understood that, within the scope of the appended claims, the invention may be practiced otherwise than as specifically described.

CLAIMS

1. A method for use in a wireless sensor network comprising at least one gateway and at least two nodes ; said method comprising the steps of:

   Performing a bi-directional authentication between nodes and between node and gateway;

   Defining and selecting an authentication header between available nodes, wherein said header contains information related to authentication, level of security for authentication and authentication messages;

   Providing authentication information with a predetermined amount of times on validation failure; and

   Forbidding an unknown entity from entering the network in the event that the validation failure exceeds the predetermined amount of time.

2. The method as claimed in Claim 1 wherein the bi directional authentication further comprising the steps of initiating authentication by means of reduce function device (RFD) via a message to full function device (FFD); sending information authentication request in a specific message from FFD to RFD; verifying authentication by RFD; providing a reply on successful verification with authentication information in a specific message from RFD and FFD; and verifying the authentication information received by FFD.

3. The method as claimed in Claim 1, wherein the step of authentication between nodes comprises the steps of inquiring node for resource availability; verifying the resources

by the RFD; and notifying the gateway on the acceptance by the node to the RFD and FFD.

4. The method as claimed in Claim 3 wherein the step notifying the gateway further comprising the steps of authenticating RFD only once per joining the network; and providing RFD confirmation and registration information to the FFD once per joining of node with the network.

5. The method as claimed in Claim 1 wherein the level of security is based on variable sizes of authentication information and various encryption systems.

6. The method as claimed in Claim 1 wherein defining the authentication header between nodes further comprising the step of checking available resources, said resources include battery level, memory level and RSSI value.

7. The method as claimed in Claim 1 wherein the method further comprising registering the nodes and gateway upon successful validation and verification.

8. The method as claimed in Claim 1 used for multi-hop wireless sensor network.

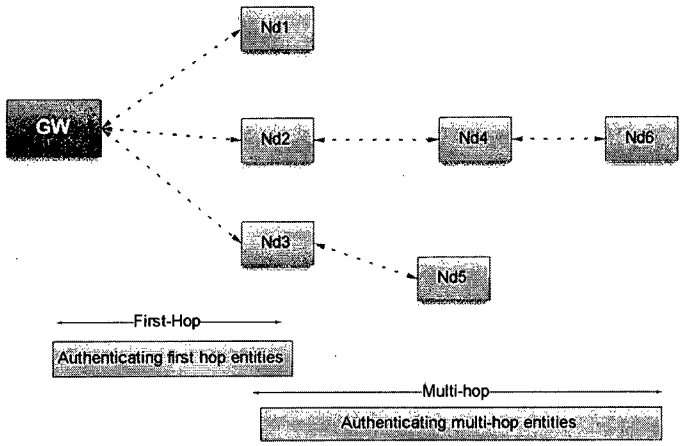
Nd1
GW
Nd2
Nd4
Nd6
Nd3
Nd5
First-Hop
Authenticating first hop entities
Multi-hop
Authenticating multi-hop entities

FIG 1

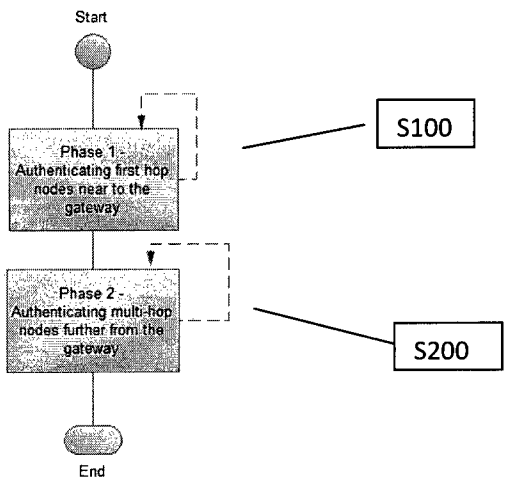
Start
Phase 1 - Authenticating first hop nodes near to the gateway
S100
Phase 2 - Authenticating multi-hop nodes further from the gateway
S200
End

FIG 2

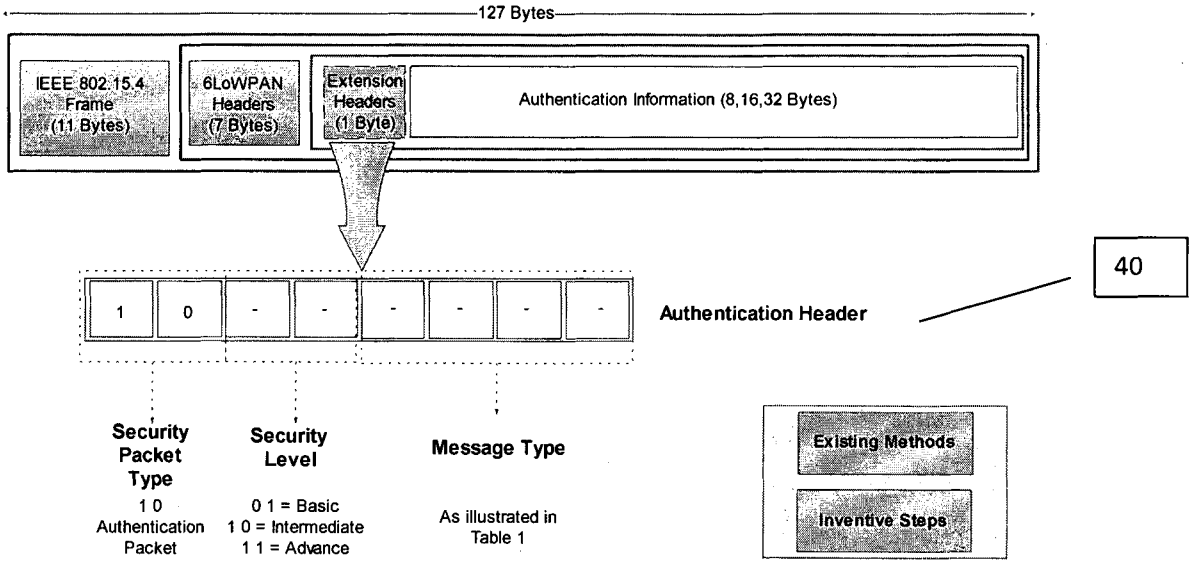
127 Bytes
IEEE 802.15.4 Frame (11 Bytes)
6LoWPAN Headers (7 Bytes)
Extension Headers (1 Byte)
Authentication Information (8,16,32 Bytes)
1
0
-
-
-
-
-
-
Authentication Header
40
Security Packet Type
1 0 Authentication Packet
Security Level
0 1 = Basic
1 0 = Intermediate
1 1 = Advance
Message Type
As illustrated in Table 1
Existing Methods
Inventive Steps

FIG 3

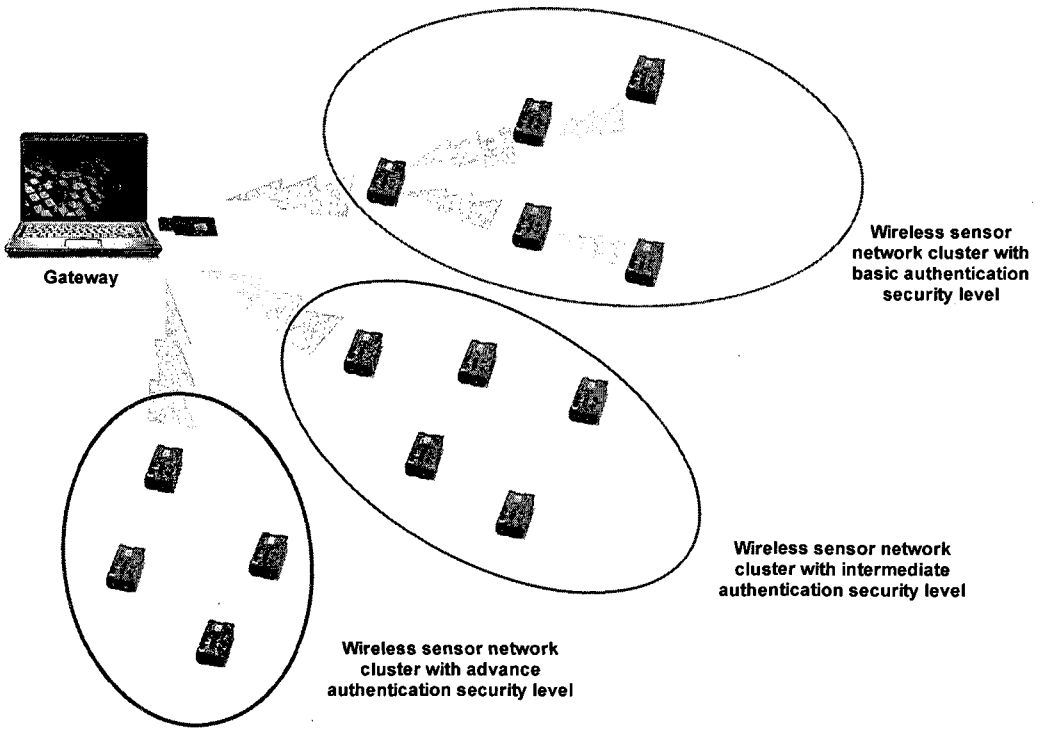
Gateway
Wireless sensor network cluster with basic authentication security level
Wireless sensor network cluster with intermediate authentication security level
Wireless sensor network cluster with advance authentication security level

FIG 4

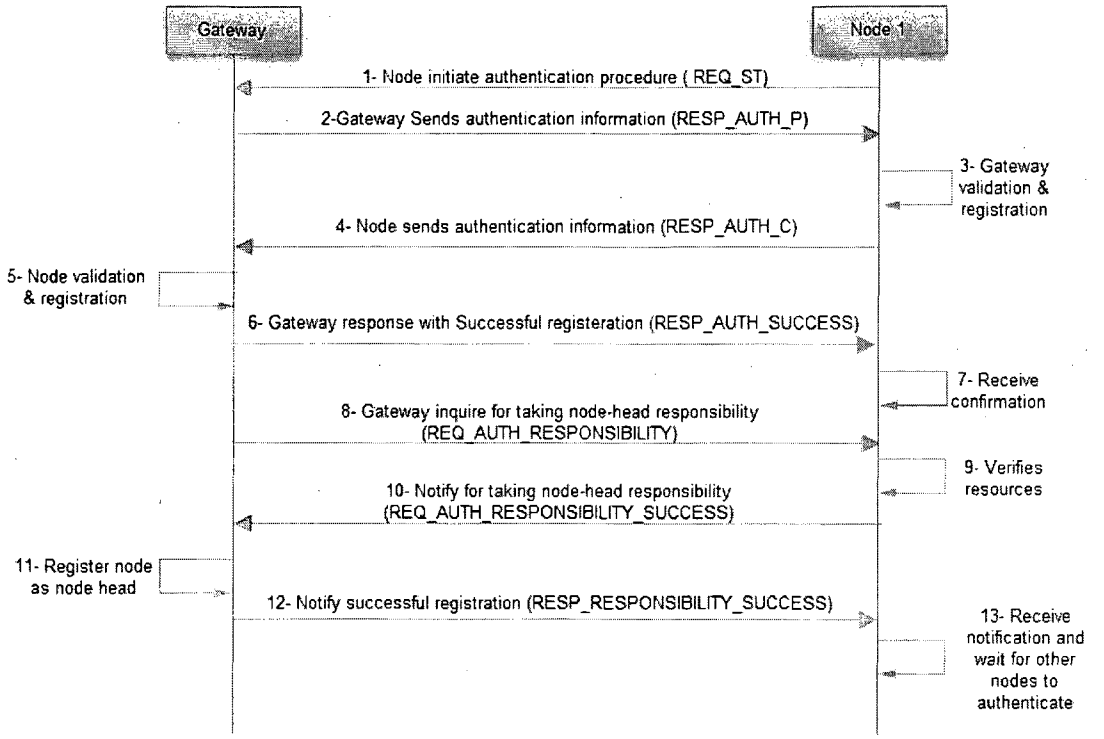
Gateway
Node 1
1- Node initiate authentication procedure (REQ_ST)
2-Gateway Sends authentication information (RESP_AUTH_P)
3- Gateway validation & registration
4- Node sends authentication information (RESP_AUTH_C)
5- Node validation & registration
6- Gateway response with Successful registeration (RESP_AUTH_SUCCESS)
7- Receive confirmation
8- Gateway inquire for taking node-head responsibility (REQ_AUTH_RESPONSIBILITY)
9- Verifies resources
10- Notify for taking node-head responsibility (REQ_AUTH_RESPONSIBILITY_SUCCESS)
11- Register node as node head
12- Notify successful registration (RESP_RESPONSIBILITY_SUCCESS)
13- Receive notification and wait for other nodes to authenticate

FIG 5

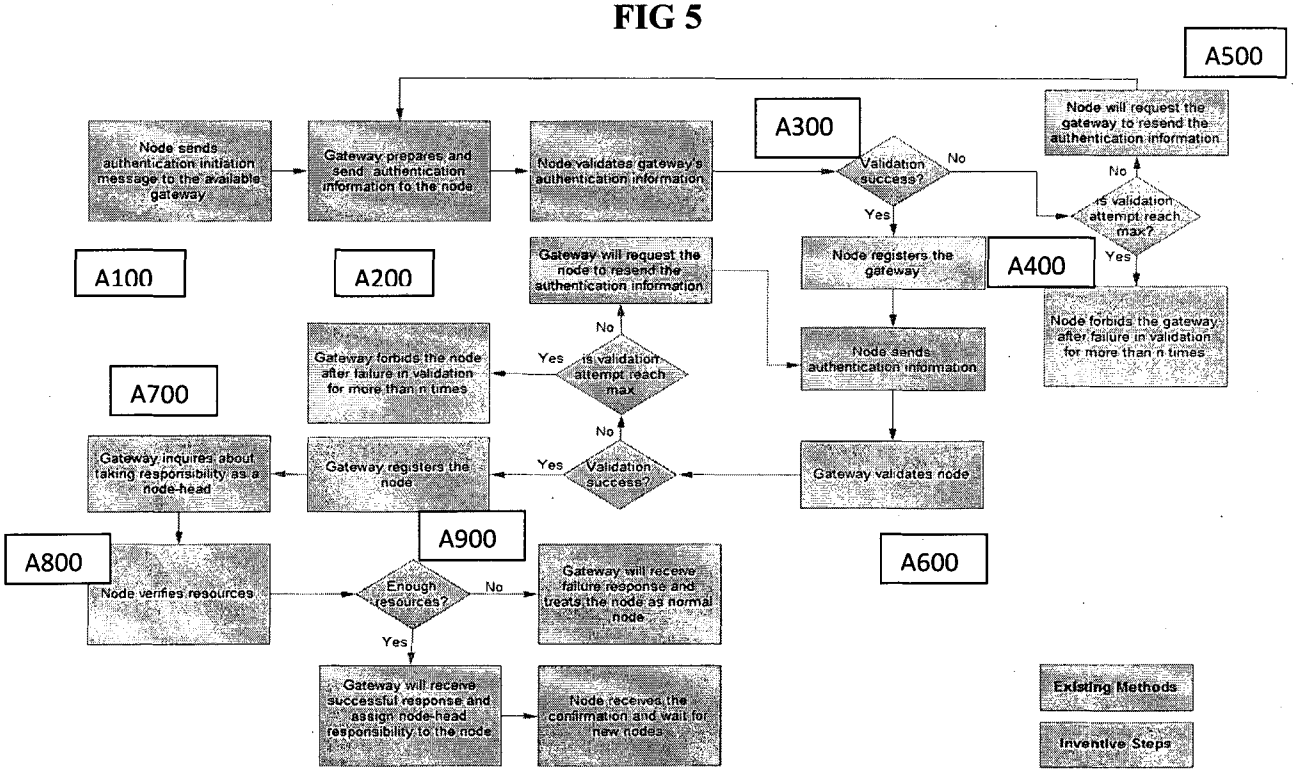
A500
A100
A200
A300
A400
A600
A700
A800
A900
Node sends authentication initiation message to the available gateway
Gateway prepares and send authentication information to the node
Node validates gateway's authentication information
Validation success?
No
Yes
Node will request the gateway to resend the authentication information
is validation attempt reach max?
Yes
Node forbids the gateway after failure in validation for more than n times
Gateway will request the node to resend the authentication information
Node registers the gateway
Node sends authentication information
Gateway validates node
Gateway forbids the node after failure in validation for more than n times
is validation attempt reach max
Gateway inquires about taking responsibility as a node-head
Gateway registers the node
Validation success?
Node verifies resources
Enough resources?
Gateway will receive failure response and treats the node as normal node
Gateway will receive successful response and assign node-head responsibility to the node
Node received the confirmation and wait for new nodes
Existing Methods
Inventive Steps

FIG 6

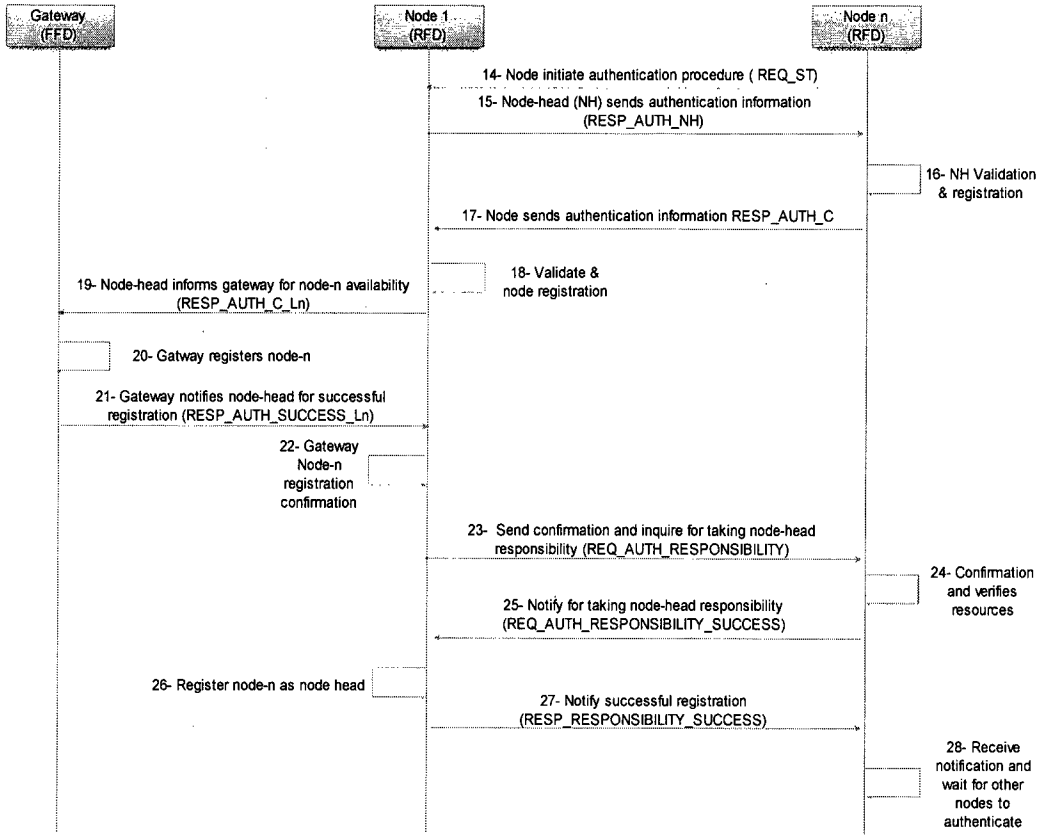
Gateway (FFD)
Node 1 (RFD)
Node n (RFD)
14- Node initiate authentication procedure (REQ_ST)
15- Node-head (NH) sends authentication information (RESP_AUTH_NH)
16- NH Validation & registration
17- Node sends authentication information RESP_AUTH_C
18- Validate & node registration
19- Node-head informs gateway for node-n availability (RESP_AUTH_C_Ln)
20- Gatway registers node-n
21- Gateway notifies node-head for successful registration (RESP_AUTH_SUCCESS_Ln)
22- Gateway Node-n registration confirmation
23- Send confirmation and inquire for taking node-head responsibility (REQ_AUTH_RESPONSIBILITY)
24- Confirmation and verifies resources
25- Notify for taking node-head responsibility (REQ_AUTH_RESPONSIBILITY_SUCCESS)
26- Register node-n as node head
27- Notify successful registration (RESP_RESPONSIBILITY_SUCCESS)
28- Receive notification and wait for other nodes to authenticate

FIG 7

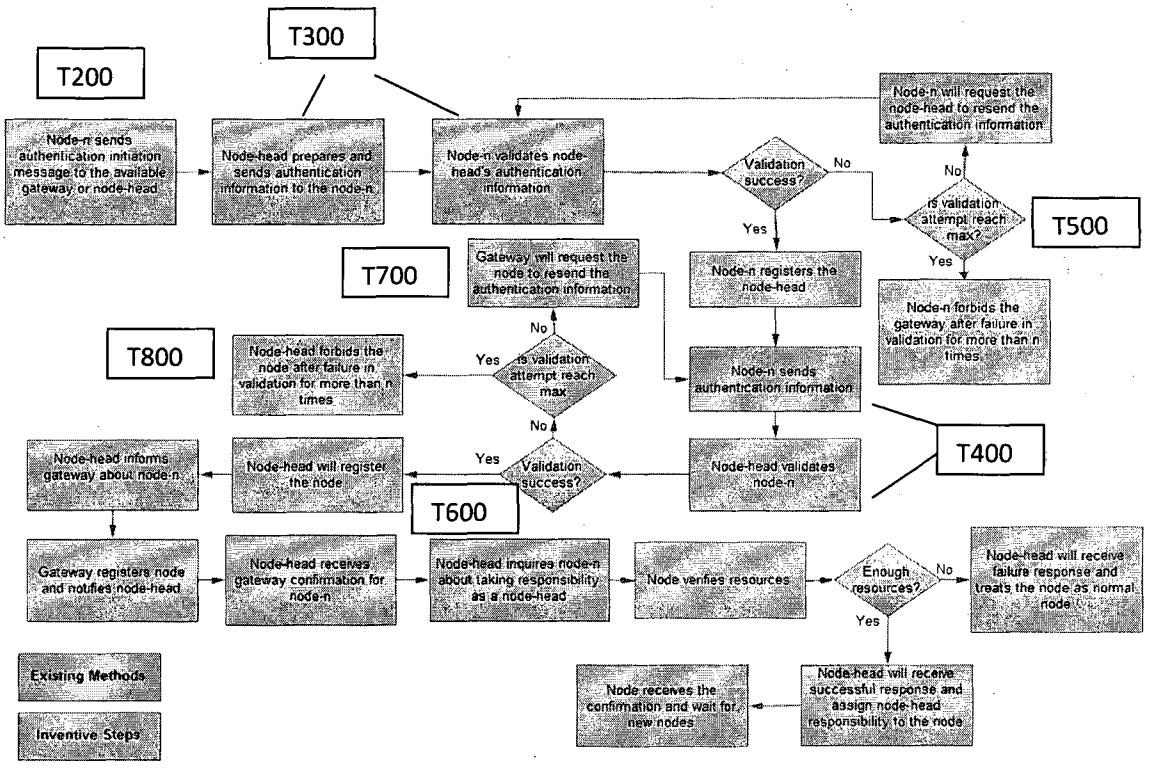
T200
T300
T400
T500
T600
T700
T800
Node-n sends authentication initiation message to the available gateway or node-head
Node-head prepares and sends authentication information to the node-n
Node-n validates node-head's authentication information
Validation success?
No
Yes
Node-n will request the node-head to resend the authentication information
is validation attempt reach max?
No
Yes
Node-n forbids the gateway after failure in validation for more than n times
Node-n registers the node-head
Gateway will request the node to resend the authentication information
Node-n sends authentication information
Node-head validates node-n
Validation success?
No
Yes
is validation attempt reach max
No
Yes
Node-head forbids the node after failure in validation for more than n times
Node-head will register the node
Node-head informs gateway about node-n
Gateway registers node and notifies node-head
Node-head receives gateway confirmation for node-n
Node-head inquires node-n about taking responsibility as a node-head
Node verifies resources
Enough resources?
No
Yes
Node-head will receive failure response and treats the node as normal node
Node-head will receive successful response and assign node-head responsibility to the node
Node receives the confirmation and wait for new nodes
Existing Methods
Inventive Steps

FIG 8

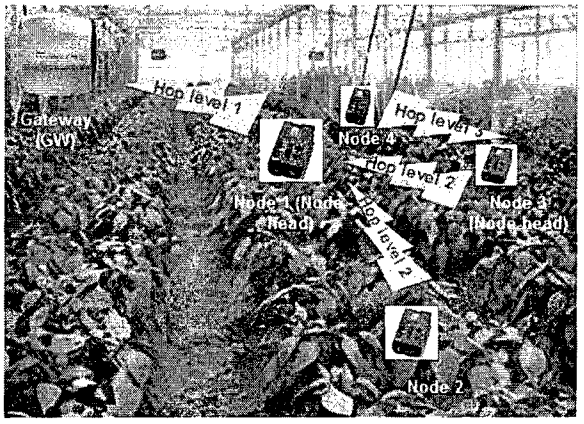
Gateway (GW)
Hop level 1
Node 4
Hop level 3
Hop level 2
Node 1 (Node-Head)
Node 3 (Node-head)
Hop level 2
Node 2

FIG 9

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference IPR/MM/D869/MIMO	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. **PCT/MY2012/000090**	International filing date *(day/month/year)* 26 April 2012	(Earliest) Priority Date *(day/month/year)* 26 April 2011

Applicant

MIMOS BERHAD et al.

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **4** sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language,** the international search was carried out on the basis of:

☒ The international application in the language in which it was filed:

☐ A translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II).

3. ☐ **Unity of invention is lacking** (See Box No. III).

4. With regard to the **title,**

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings,**

a. the figure of the **drawings** to be published with the abstract is Figure No. **1**

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2012/000090

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) H04L 9/32 (2006.01) H04K 1/00 (2006.01)

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)

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 practicable, search terms used)
WPI, EPODOC, INSPEC with keywords: authentication, bi-directional, security level, sensor, signal strength, time, encrypt, forbid, RFD and similar terms.

Google Patents and Google Scholar searched with similar keywords as above.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] 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 application or patent 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
28 September 2012	28 September 2012

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
Email address: pct@ipaustralia.gov.au
Facsimile No.: +61 2 6283 7999

Authorised officer

Dr. Rasika Perera
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. 0262833116

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/MY2012/000090**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0332831 A1 (SHON et al.) 30 December 2010 See the whole document in particular the abstract, figures 1, 3C, 4, 5, 6, 8, paragraphs 0025, 0040-0046, 0051, 0055-0056, 0062-0065, 0070, 0072, 0076-0081, 0088-0098, 0100-0101.	1-8
X	US 2007/0116292 A1 (KURITA et al.) 24 May 2007 See the whole document in particular the abstract, figures 1, 5, 7, paragraphs 0009-0018, 0038, 0062-0066, 0105-0123, 0131, and 0143-0160.	1-7

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/MY2012/000090**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2010/0332831 A1	30 Dec 2010	KR 20110000334 A	03 Jan 2011
		US 2010332831 A1	30 Dec 2010
US 2007/0116292 A1	24 May 2007	CN 101031113 A	05 Sep 2007
		CN 101031113 B	10 Nov 2010
		JP 2007142820 A	07 Jun 2007
		JP 4435076 B2	17 Mar 2010
		US 2007116292 A1	24 May 2007
		US 7797537 B2	14 Sep 2010
		US 2010325713 A1	23 Dec 2010

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.