



- (51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) International Application Number:
PCT/IB2012/052867
- (22) International Filing Date:
7 June 2012 (07.06.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
11169394.1 10 June 2011 (10.06.2011) EP
- (71) Applicant (for all designated States except US):
KONINKLIJKE PHILIPS ELECTRONICS N.V.
[NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **GARCIA MORCHON, Oscar** [ES/DE]; c/o High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL). **GÖRGEN,**

Daniel, Martin [DE/NL]; c/o High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL). **SCHENK, Tim, Corneel, Wilhelmus** [NL/NL]; c/o High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL). **ESPINA PEREZ, Javier** [ES/NL]; c/o High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL). **AOUN, Marc** [LB/NL]; c/o High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL).

- (74) Agents: **VAN EEUWIJK, Alexander, Henricus, Walterus** et al.; High Tech Campus, Building 44, NL-5656 AE Eindhoven (NL).

- (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,

[Continued on next page]

- (54) Title: SECURE DATA TRANSMISSION TO NETWORK NODES IN A NETWORK

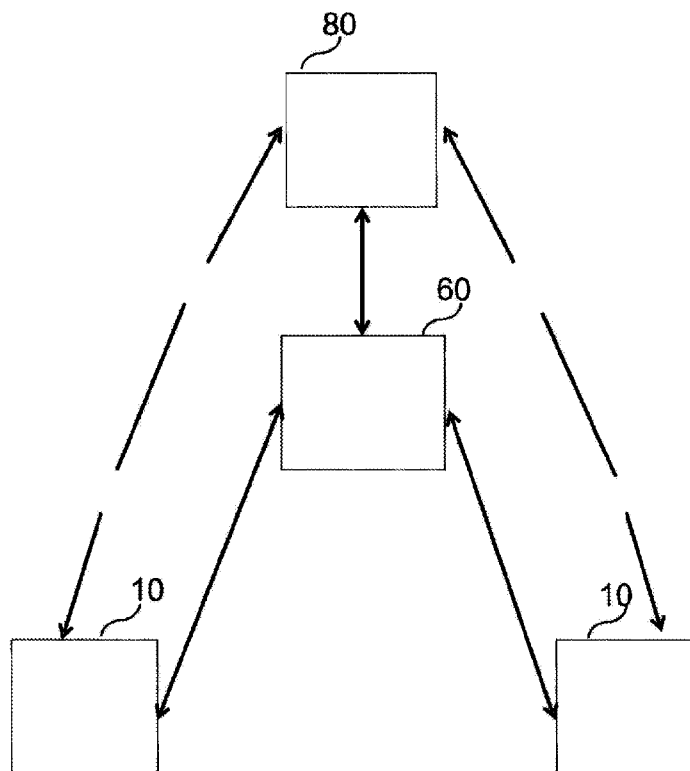


Fig. 5

(57) Abstract: For secure data transmission to a node of a network providing minimized communication overhead and improved protection of the network against counterfeiting, a system, a control unit and a method are provided, wherein a segment controller provides information from a service center to at least one node, with the node and the segment controller being capable of mutual authentication and the node (10) being further adapted to verify an authorization of the segment controller (60) and to accept the information in case of successful verification.



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

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))

SECURE DATA TRANSMISSION TO NETWORK NODES IN A NETWORK

FIELD OF THE INVENTION

The invention relates to a system, a control unit and a method for secure data transmission to a node of a network.

BACKGROUND OF THE INVENTION

Recently, wireless mesh networks attract more and more attention, e.g. for remote control of illumination systems, building automation, monitoring applications, sensor systems and medical applications. In particular, a remote management of outdoor luminaires, so-called telemanagement, becomes increasingly important. On the one hand, this is driven by environmental concerns, since telemanagement systems enable the use of different dimming patterns, for instance as a function of time, weather conditions or season, allowing a more energy-efficient use of the outdoor lighting system. On the other hand, this is also driven by economical reasons, since the increased energy efficiency also reduces operational costs. Moreover, the system can remotely monitor power usage and detect lamp failures, which allows for determining the best time for repairing luminaires or replacing lamps.

Current radio-frequency (RF) based wireless solutions use either a star network topology or a mesh network topology. In a star network, a central controller has a direct wireless communication path to every node in the network. However, this typically requires a high-power/high-sensitivity base-station-like central controller to be placed at a high location (e.g. on top of a building), which makes the solution cumbersome to deploy and expensive. In a mesh network, the plurality of nodes does in general not communicate directly with the central controller, but via so-called multi-hop communications. In a multi-hop communication, a data packet is transmitted from a sender node to a destination node via one or more intermediate nodes. Nodes act as routers to transmit data packets from neighboring nodes to nodes that are too far away to reach in a single hop, resulting in a network that can span larger distances. By breaking long distances in a series of shorter hops, signal strength is sustained. Consequently, routing is performed by all nodes of a mesh network deciding, to which neighboring node the data packet is to be sent. Hence, a mesh network is a very robust and stable network with high connectivity and thus high redundancy and reliability.

In Figure 1, a typical wireless network with mesh topology is shown. The wireless network comprises of a central controller 60 and a plurality of nodes 10 (N) being connected among each other by wireless communication paths 40 in a mesh topology. The wireless communication paths 40 between the nodes 10 can be constituted by RF transmissions. For this, the nodes 10 and the central controller 60 can comprise a transceiver for transmitting or receiving data packets via wireless communication paths 40, e.g. via RF transmission. In the backend, a service center 80 is situated and serves for system management. This entity normally communicates with one or more wireless networks over a third party communication channel 70, such as the Internet or mobile communication networks or other wired or wireless data transmission systems. In particular, the service center 80 communicates with a central controller 60 of a corresponding network as a commissioning tool in charge of controlling or configuring this network. In case of a lighting system or any other large wireless network, a network can also be divided into segments, so that a node 10 belongs to exactly one segment having one segment controller 60. Therefore, the terms "segment controller" and "central controller" should be seen as exchangeable throughout this description.

In general, any node 10 of the mesh network can communicate with the service center 80 via the segment controller 60. However, in some situations, high security standards have to be fulfilled in order to provide basic security services. An example is protection against counterfeiting, i. e. preventing non-authorized nodes from joining the overall system. Another example refers to enabling services from the service centre, e. g. when updating dimming patterns of luminaire nodes in a lighting system or when transmitting other configuration or commissioning information, in this case, it is important to ensure that only authorized nodes 10 of the network receive the information. In addition, it is important that only the service center 80 of the system is authorized to send such information to the nodes 10. Thus, on the one hand, the nodes 10 must be identified by the system in order to avoid fraud and infiltration of the network by non-authorized nodes. On the other hand, the identity of the system must be verified by the nodes 10 in order to avoid theft of node credentials by a hostile entity pretending to be the service center 80. Therefore, a two-way authentication is required.

Traditional end-to-end security protocols that allow end-to-end commissioning require the interactive exchange of messages between the service center 80 and the nodes 10, e.g., based on a challenge-response authentication handshake. Although such a procedure provides high security, it poses severe requirements regarding the usage of the GPRS link 70

as shown in fig. 1 or on the number of operations performed in the backend at the service center 80. Therefore, common basic security protocols enabling such mutual authentication and secure transfer of configuration information require end-to-end connectivity between the service center 80 and the single network nodes 10. However, in particular for mesh networks, this cannot always be guaranteed, since the service center 80 may be offline and not always available. Moreover, end-to-end handshakes between the service center 80 and each individual node 10 are too expensive with respect to network resources, resulting in large communication overhead. Hence, it is desired to find a protocol for secure data transmission between the service center 80 and a single node 10 providing a reasonable trade-off between security and operational needs suitable for the respective application.

WO 2010/023619 A1 relates to commissioning a wireless network, wherein a network device being part of the network communicates with a device joining the network in a commissioning mode and provides joining information to the joining device, which is needed for network communication.

SUMMARY OF THE INVENTION

In view of above disadvantages and problems in the prior art, it is an object of the present invention to provide a system, a control unit and a method for secure transmission of data to a node of a wireless network minimizing communication overhead, while providing protection of the network against counterfeiting.

The invention is based on the idea to transmit information from a service center to a network node of a network, e.g. a wireless network, via an intermediate entity, e.g. a segment controller, which is authenticated and authorized by the service center. When the node and the intermediate entity have mutually authenticated each other and the node has verified the authorization of the intermediate entity, the node accepts the received information. It is to be understood that the service center as well as the controlling device or segment controller may also be represented by a certain network node, respectively. Mutual authentication may correspond to a mutual security handshake, for instance a challenge-response based handshake, or the like. During the mutual authentication process, both parties might agree on a common key, so that a secure communication channel is set up between the involved entities. This idea may be particularly suited for commissioning nodes of a wireless network from the backend. Thus, the configuration of single nodes may be performed on behalf of the segment controller without involving expensive end-to-end handshakes between

the service center and the single nodes, while exhibiting security properties equivalent to a pure end-to-end handshake.

According to one aspect of the present invention, a system for secure data transmission to a node of a wireless network is provided. The system may comprise at least one node, at least one segment controller and a service center. The service center may provide information for at least one of the nodes to the corresponding segment controller, e.g. configuration information, commissioning information or update information. This information may be provided from the segment controller to the node during or after mutual authentication. The node may accept the information after successful authentication and after verifying that the segment controller is authorized by the service center. The verification of the authorization of the segment controller by the node may be based on a security key, which is known to the service center and the node, but not to the segment controller. For instance, the information provided by the service center may be encoded based on this security key. Hence, in the example of a configuration or commissioning procedure, the node may implement the received information only after successful authentication and verification. Therefore, means are provided enabling secure data transmission, e.g. for commissioning or service provisioning. Due to the verification of the authorization of the segment controller by the node and due to the mutual authentication between the segment controller and the node, an end-to-end handshake between the service center and the node may be mimicked, guaranteeing secure transfer of information, while waste of network resources is avoided. Moreover, dedicated node security domains may be created, thus preventing the theft of joining credentials of the network and protecting against counterfeiting by ensuring that a node cannot run in operational mode if it has not been authenticated.

Preferably, during or after mutual authentication, a session key is derived by the entities involved in the mutual authentication process, so that both entities have the same session key available. This session key may be derived based on at least one of the security keys associated to the respective entities and random data. For instance, the session key generated during mutual authentication between the node and the segment controller may be a function of the node key and/or of the key of the segment controller. Preferably, the generation of the session key is also based on an identification number of the session, i. e. for one communication process such as a security handshake or other data transfer, so that the session key is only valid for this session. This identification number may be any random number associated to the session. The key generation may be based on symmetric-key cryptography or asymmetric-key cryptography, e. g. using a hash message authentication

code (HMAC) or a cipher message authentication code (CMAC). Therefore, the session key may not only be limited to certain entities, but also to a certain time slot or communication. By means of the session key, a secure communication channel between two entities may be set up. Thus, only devices with the correct session key may be capable of participating in the communication. By locally generating the session key at the respective entities, eavesdropping on the session key may be prevented.

In a further embodiment, the service center may be configured to provide a session-limited security key of the node to the segment controller. In this embodiment, the segment controller may generate the session key based on the session-limited security key of the node. In addition, the segment controller may use a security key associated to itself and/or to the network or system. The session-limited security key of the node may be generated by the service center using a session identity number, specific configuration parameters, and the security key of the node, which may be known to the service center. Therefore, the segment controller may be only informed about a session-limited security key of the node, which can be considered as a coded security key of the node, but not of the general security key of the node. Thus, the service center may have to allow communication sessions between the segment controller and the node by providing the segment controller with the corresponding session-limited security key of the node. This further increases the security of the network. Moreover, since only a session-limited key of the node is transmitted, eavesdropping on this key does not allow unlimited access to the corresponding node.

The service center may know at least one of the security keys of itself, of the segment controller and of the node. However, it is preferred that the service center knows at least the security keys of the segment controller and the node. In contrast, the segment controller and the node may only know their own security keys.

In a preferred embodiment of the present invention, the service center may be adapted to commission and/or to configure the segment controller. For this, the service center and the segment controller may be involved in a mutual authentication process, such as an end-to-end security handshake. After successful verification of each other's identities, the service center may commission and/or configure the segment controller, thus authorizing the segment controller for communication with network nodes. In one example, the service center may be adapted to authorize the segment controller for commissioning and/or controlling the nodes. Hence, the service center may activate the segment controller as a controlling device for one or more nodes of the network. In this embodiment, the segment controller may thus be directly configured by the service center, while the node may be

configured indirectly by the service center via the segment controller after successful configuration of the segment controller by the service center. Here, only the first step requires direct connectivity with the service center. Thus, by configuring nodes via an intermediary entity, i.e. the segment controller, the required communication between the service center and the node is decreased, so that even a configuration of a large network comprising a plurality of nodes can be performed without much effort for the service center.

Before providing the information to the node, the segment controller may verify that the node is the actual addressee of the information. Hence, the segment controller may provide the information to the node after mutual authentication between the segment controller and the node. Alternatively, the segment controller may provide the information to the node before completing the authentication process, e.g. during or even before the mutual authentication. This may be preferred in a large network using multi-hop transmissions, e.g. if the information is coded anyway using the security key of the node, so that eavesdropping or unauthorized modification of the information is prevented. Likewise, the service center may provide the information for the node to the segment controller after or during mutual authentication between the service center and the segment controller.

After accepting the information, the node may transmit a confirmation message via the segment controller to the service center. This confirmation message may be encoded twice, first with a common key associated to the segment controller and the node and second using a common key associated to the service center and the node. By these means, the segment controller may decode the confirmation message and verify the authenticity thereof. Then, the segment controller may forward the single-coded confirmation message to the service center. By these means, the service center may verify that the node has correctly received the information and/or that the node has correctly performed a requested action, e.g. a configuration process.

Preferably, messages between the segment controller and the service center are transmitted in batches. For instance, if the service center provides information for a plurality of nodes, the service center may transmit a batch of messages including the information for the respective nodes to the segment controller. Likewise, if the segment controller receives confirmation messages from a plurality of nodes, the segment controller may collect the confirmation messages and transmit the confirmation messages in one batch to the service center. By these means, traffic via the third party communication channel may be further reduced. Moreover, in a large network, information provided by the service center may be the same for several nodes. For instance, in a lighting system, the configuration information will

be the same for most of the luminaire nodes. Then, the service center may provide the configuration information to the segment controller, so that the segment controller may distribute the information to the respective nodes in an individual way.

In a further embodiment, at least one threshold time may be set for defining a maximum time period allowed between two predefined actions, e. g. between transmission of two predefined messages. The threshold time may be set at the at least one of the node, the segment controller and the service center. Preferably, a threshold time is set for messages exchanged during an authentication process. For instance, the time for successful authentication between the segment controller and the node may be limited. Similarly, a threshold time may be defined at the service center between transmission of the information to the segment controller and receipt of the confirmation message of the node. In case that the threshold time is exceeded, an alarm may be triggered and/or reconfiguration may be requested. By these means, replay messages may be suppressed, wrong configurations dropped, or attempts for non-authorized configuration stopped.

In a further embodiment, the node may be configured such that information from the service center may only be accepted during a specified phase. For instance, configuration information and thus configuration of the node may only be allowed during a predefined configuration phase. By means of such a phase-aware operation of the node, the network security can be further increased. Similarly, the segment controller and/or the service center may be aware of a current network phase.

In a preferred embodiment, messages between the segment controller and the node are encoded using a common security key associated to both the node and the segment controller. Alternatively or additionally, messages between the segment controller and the service center may be encoded using a common security key associated to both the service center and the segment controller. Alternatively or additionally, messages exchanged between the node and the service center via the segment controller may be encoded using the security key of the node, which may correspond to the security key of the node. Thus, when the service center provides the information for the node to the segment controller, the information may be encoded using the security key of the node (or any other key common to the service center and the node), which is not shared with the segment controller. By these means, the segment controller or hostile attackers cannot change the information.

In a preferred embodiment, the nodes of the network correspond to luminaire nodes of a lighting system. Thus, the system according to the present invention may be used for telemanagement of a lighting system such as an outdoor or street lighting system. By

these means, the restricted resources of such a lighting system are met, while providing secure data transfer.

According to another aspect of the present invention, a control unit for secure data transmission to a node of a wireless network is provided. The control unit comprises an authentication unit adapted to mutually authenticate the node and a segment controller and to verify an authorization of the segment controller, wherein information provided from a service center via the segment controller is accepted in case of successful verification. Therefore, the control unit is adapted to realize features as described above for embodiments of a system according to the present invention.

According to a further aspect of the present invention, a method for secure data transmission to a node of a wireless network is provided, comprising the steps of mutual authentication of a node and a segment controller, verification of an authorization of the segment controller by the node and acceptance of the node of information provided from a service center via the segment controller in case of successful verification. Therefore, the method according to the present invention is adapted to be performed by the system or the control unit according to any one of the above-described embodiments of the present invention.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter. The invention will be described in more detail with respect to exemplary embodiments that are illustrated by the accompanying figures. However, the invention is not limited to these exemplary embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

In the figures:

Fig. 1 illustrates an example of a wireless mesh network;

Fig. 2 shows a flow diagram for illustrating a configuration process of a node by a service center via a segment controller according to an embodiment of the present invention;

Fig. 3 shows a flow diagram of a process for configuring a segment controller according to an embodiment of the present invention;

Fig. 4 shows a flow diagram of a process for configuring a node according to an embodiment of the present invention;

Fig. 5 illustrates security connections between nodes, a segment controller and a service center according to an embodiment of the present invention; and

5 Fig. 6 shows a control unit for a node according to an embodiment of the present invention.

DETAILED DESCRIPTION

Preferred applications of the present invention are actuator or sensor networks such as lighting systems, e.g., outdoor lighting systems (e.g. for streets, parking and public
10 areas) and indoor lighting systems for general area lighting (e.g. for malls, arenas, parking, stations, tunnels etc.), smart energy systems, or pervasive healthcare systems. In the following, the present invention will be explained further using the example of an outdoor lighting system for street illumination, however, without being limited to this application. In the field of lighting control, the telemanagement of outdoor luminaires via radio-frequency
15 network technologies is receiving increasing interest, in particular solutions with applicability for large-scale installations with segments of above 200 luminaire nodes. Since radio frequency (RF) transmissions do not require high transmission power and are easy to implement and deploy, costs for setting up and operating a network can be reduced. However, the data packet transmission may alternatively use infrared communication, free-
20 space-visible-light communication or power line communication.

In a telemanagement system for lighting control, the number of luminaire nodes 10 is extremely high. Hence, the size of the network is very large, especially when compared to common wireless mesh networks, which typically contain less than 200 nodes. In addition, the nodes 10 typically have limited processing capabilities due to cost
25 considerations, so that processing and memory resources in the luminaire nodes 10 will be limited. Thus, security measures and communication protocols for transmitting data packets between single nodes 10 should consider the limited resources for efficient and secure data packet transmission. Finally, compared to other so-called ad-hoc mesh networks, the telemanagement system for an outdoor lighting control network is stationary, i.e. the
30 luminaire nodes 10 do not move. Since the luminaire nodes 10 (e.g. the lamp poles) are stationary, node positions will not change over time. Thus, the physical positions of the nodes 10, for instance GPS-coordinates or other position data, may be known in the system, enabling geographic or position-based routing using pre-programmed or predefined positions,

so that no GPS receiver is required in the single nodes 10. In addition, the nodes 10 do not need to send position information updates to other nodes 10.

According to one embodiment of the present invention, the service center 80 provides information to a network node 10 via an authenticated segment controller 60. For mutual authentication or verification of identities, in general, a mutual security handshake or any other end-to-end security protocol can be used. The security handshake should also allow for agreement on a common key associated to the involved entities in order to allow for the establishment of a secure communication channel. In the following, embodiments of the present invention are explained using the example of configuration information, i.e. wherein the service center 80 configures the node 10 via the segment controller 60. However, any kind of data other than configuration information can be transmitted in this way. Therefore, the present invention is not limited to configuration processes.

In fig. 2, a process of configuring a node of a wireless network by the service center 80 is described. As mentioned before, the nodes 10 of the network are associated to a segment controller 60. Therefore, before configuring the node 10 from the backend, the segment controller 60 and the service center 80 verify the identity of each other in a mutual authentication process (S310). This mutual authentication process can relate to a challenge-response based handshake or any other end-to-end security protocol. During this authentication process, a common security key can be generated at both the service center 80 and the segment controller 60, so that a secure communication channel can be set up. Optionally, e.g., if this is the first contact between the segment controller 60 and the service center 80 in a commissioning phase, the service center 80 may configure the segment controller 60. Thus, the service center 80 may activate operational functions of the segment controller 60, i.e. activate the segment controller 60 as a controlling device of the network or of the network nodes 10 (S320). After successful mutual authentication and setup of the secure communication channel (S310), the service center 80 transmits a message including configuration information for a node 10 to the segment controller 60 (S330). This message may be encoded using a common key associated to the segment controller 60 and the service center 80. If the service center 80 knows a security key of the node 10, the configuration information for the node 10 may also be encoded using this security key of the node 10. In the next step S340, the segment controller 60 and the node 10 verify the identity of one other in a second mutual authentication process. Again, this authentication process may include the generation of a common security key to, e.g., secure the link based on common keys, random data and configuration parameters of segment controller and node. When involving the

exchange of several messages, the configuration information can be transmitted to the node 10 in the beginning of the mutual authentication process. After having received the message including the configuration information, the node 10 verifies the authenticity of the message, e.g. using its own security key (S350). This may include verifying that the message originates from the service center 80 and that the segment controller 60 is authorized by the service center 80 to provide the message to the node 10. After successful verification of the authenticity of the message and successful mutual authentication with the segment controller 60, the node 10 accepts the received message and uses the configuration information for configuration (S360). After completed configuration, the node 10 may optionally send a configuration confirmation via the segment controller 60 to the service center 80 (S370). Preferably, the configuration confirmation is encoded twice, i.e. using the common key associated to the node 10 and the segment controller 60 and using the security key of the node 10, which is not known to the segment controller 60. By means of the common key associated to the node 10 and the segment controller 60, the segment controller 60 can verify the authenticity of the configuration message (S380). However, the segment controller 60 cannot change the configuration confirmation message, since the segment controller 60 does not know the second coding, i.e. the security key of the node 10. That is, the segment controller 60 can check that the configuration confirmation comes from the actual node 10, but it cannot check the content of the configuration confirmation message. Then, in step S390, the segment controller 60 transmits the configuration confirmation message to the service center 80, so that the service center 80 can verify based on the security key of the node 10 that it is the correct node 10 that was configured and that the node 10 has been successfully configured with the correct parameters.

Since the segment controller 60 has direct access to the service center 80, a correct and secure commissioning or configuration of the segment controller 60 is fundamental. In general, any party accessing the service center 80 should be correctly authenticated and authorized and the corresponding communication channel should be secured. Moreover, the segment controller 60 is involved in all interactions between the service center 80 and the nodes 10 of the network. Therefore, the device involved in that link should be a trusted device. This is even more important for the example of configuring the nodes 10, i.e. when the segment controller 60 has to represent the service center 80 in some configuration tasks, such as node commissioning or the like. Hence, a correct and secure authentication of the segment controller 60 by the service center 80 is prerequisite.

In fig. 3, an exemplary embodiment for the mutual authentication process between the segment controller 60 and the service center 80 is shown in further detail. In the following embodiments, it is assumed that the service center 80 knows the security key of the segment controller 60 and of the network node 10, i.e. K_{segment} and K_{node} . In contrast, the segment controller 60 and the network node 10 only know their own security keys K_{segment} and K_{node} , respectively. In general, a mutual challenge-response based handshake for mutual authentication is based on some keying material, which is known to both entities involved in the handshake, such as the security key of the segment controller 60 K_{segment} .

Therefore, as a first step in fig. 3, the segment controller 60 transmits a message M1 to the service center 80 including a random number r_{segment} generated at the segment controller 60. The service center 80 answers by transmitting a message M2 including a further random number r_{service} generated at the service center 80. Based on these random numbers r_{segment} and r_{service} as well as on the security key K_{segment} of the segment controller 60, the segment controller 60 generates a session key K_{session} . For instance, the session key K_{session} may be generated using the following expression:

$$K_{\text{session}} = \text{HMAC}(\text{key} \parallel r_{\text{service}} \parallel r_{\text{segment}}, K_{\text{segment}})$$

Here, two vertical lines represents concatenation. Thus, the session key K_{session} may be a hash message authentication code function of the random numbers r_{segment} and r_{service} and the security key K_{segment} of the segment controller 60. The function can add further elements such as the identities of the involved parties. Alternatively, a symmetric key cryptography can be used for the authentication process, e.g. based on a cipher message authentication code CMAC. After generating the session key K_{session} , the segment controller 60 transmits a third message M3 to the service center 80. The message M3 can be an output of a function that is used as an identification token. For instance, the message M3 is based on a function of following parameters: identity $\text{Id}_{\text{segment}}$ of the segment controller 60, identity $\text{Id}_{\text{service}}$ of the service center 80 and the random numbers r_{service} and r_{segment} . Furthermore, the message M3 is encoded using the session key K_{session} , which is a common security of the segment controller 60 and the service center 80 limited to this handshake or session. Thus, a function for the message M3 may correspond to the following expression:

$$\text{HMAC}(\text{Com1} \parallel \text{Id}_{\text{segment}} \parallel \text{Id}_{\text{service}} \parallel r_{\text{service}} \parallel r_{\text{segment}}, K_{\text{session}})$$

Upon receipt of the message M3, the service center 80 also generates the session key K_{session} using the same formula as the segment controller 60. By these means, the service center 80 can verify the authenticity of the message M3 using the session key K_{session} . If the verification is successful, the service center 80 can add the segment controller 60 to a list of authorized

controlling devices and associate the segment controller 60 to the given network. Then, the service center 80 responds with a message M4, which is also a function of the identity $Id_{service}$ of the service center 80, of the identity $Id_{segment}$ of the segment controller 60 and of the random numbers $r_{segment}$ and $r_{service}$. Again, the message M4 is encoded using the session key $K_{session}$. Therefore, the message M4 can be based on the following expression:

$$HMAC(Com2 || Id_{service} || Id_{segment} || r_{segment} || r_{service}, K_{session})$$

Verification by the segment controller 60 occurs after reception and successful verification of the message M4. Optionally, for instance, if this is a commissioning handshake for configuring the segment controller 60, the segment controller 60 can be activated by the message M4 and include a security policy that moves to it to an operational state. In this state, the segment controller 60 can perform controlling functionalities such as commissioning network nodes 10 or transmitting messages between the service center 80 and the network nodes 10. It should be noted that the segment controller 60 could comprise two modules 60a and 60b. In this case, the handshake occurs between the service center 80 and the module 60b via the module 60a of the segment controller 60.

In the above-described authentication process, a common authentication handshake is modified by generating a session key $K_{session}$ specific for the service center 80 and the segment controller 60, so that the session key $K_{session}$ can be used to secure the communication link between these entities. Non-authorized traffic may be dropped. Thus, a successful authentication process provides both parties with an implicit proof that the same session key $K_{session}$ has been generated at the service center 80 and at the segment controller 60. By means of the mutual authentication and secure channel establishment between the service center 80 and the segment controller 60, the requirements for operation of the secure data transmission protocol according to the present invention are met.

In fig. 4, the operation of a secure data transmission protocol according to an embodiment of the present invention is shown. Again, the protocol is exemplified using a commissioning procedure. In the example shown, the segment controller 60 exchanges four messages N2, N3, N4 and N5 with the node 10, which encapsulate the messages m1, m2, m3 and m4. Therefore, this process resembles an authentication process or end-to-end handshake between the service center 80 and the node 10. The data exchange of the messages N2 to N5 between the segment controller 60 and the node 10 is embedded in the exchange of two sets of messages N1 and N6 between the service center 80 and the segment controller 60. The first set of messages N1 is transmitted from the service center 80 to the authorized segment controller 60 (e.g. as described above) and serves to provide the segment controller 60 with

information required for configuring one or more network nodes 10. The second set of messages N6 is transmitted from the segment controller 60 to the service center 80 and contains a configuration confirmation of the configured nodes 10.

Now, the process shown in fig. 4 is described in further detail. In general, the service center 80 is aware of the security keys K_{segment} and K_{node} of the segment controller 60 and the node 10, respectively. In contrast, the segment controller 60 and the node 10 only know their own security keys K_{segment} and K_{node} , respectively. After the segment controller 60 has been successfully authenticated and authorized, the service center 80 generates a random number for a session number r_{session} . Using the session number r_{session} and the security key K_{node} of the node, a session key $K_{\text{node_session}}$ is generated. For instance, the session key $K_{\text{node_session}}$ may be generated using a message authentication code function as in the following expression:

$$K_{\text{node_session}} = \text{MAC}(r_{\text{session}}, K_{\text{node}})$$

The above r_{session} can be generated by using as session a derivative of K_{session} , $\text{HMAC}(\text{random}, K_{\text{session}})$, where K_{session} is the key bound to service center and segment controller specific to the previous handshake and random is a random number. In this way, it can be ensured that $K_{\text{node_session}}$ is linked to the session established between the service center and the segment controller. Then, the service center 80 transmits to the segment controller 60 a message N1 including the session key $K_{\text{node_session}}$, the session number r_{session} and a message m1, which includes information for the node 10 encoded with the security key K_{node} (or a derivative of it, e.g., $\text{MAC}(\text{random}, K_{\text{node}})$ where *random* is a random number to be provided to the node) of the node 10. The information of the message m1 refers to configuration parameters for the node 10 and a security key $K_{\text{seg_syst_sess}}$ associated to the segment controller 60 as well as to the system and the current session.

For instance, the session key $K_{\text{seg_syst_sess}}$ can be generated according to the following expression:

$$K_{\text{seg_syst_sess}} = \text{MAC}(K_{\text{segment}} \parallel \text{system} \parallel r_{\text{session}})$$

By these means, the node 10 can be informed about the identity of the segment controller. Hence, in one example, the message m1 may correspond to the following expression:

$\text{AE}(\text{Com1} \parallel \text{Id}_{\text{service}} \parallel \text{Id}_{\text{segment}} \parallel \text{Id}_{\text{node}} \parallel r_{\text{session}} \parallel K_{\text{seg_syst_sess}} \parallel \text{config. Params}, K_{\text{node}})$,

wherein Com1 refers to the message number, Id refers to the identity or address of the respective entity, config. params denotes configuration parameters and AE denotes an authenticated encryption function using K_{node} (or a key derived from it, e.g., as

$MAC(random, K_{node})$ where *random* is a random number to be provided to the node). In addition, the message N1 can be encoded using a common security key associated to the service center 80 and the segment controller 60, such as the session key $K_{session}$ or any other security key based on the security key $K_{segment}$ of the segment controller 60.

- 5 After having safely received the message N1 from the service center 80, the segment controller 60 transmits a message N2 to the node 10 including the session number $r_{session}$ and the message m1. In other words, the segment controller 60 forwards the encoded message m1 without modifying it. Upon receipt of the message N2, the node 10 decrypts and verifies the authenticity of the message m1 using the corresponding security key K_{node} (or a
10 key derivated from it). Then, the node 10 stores the configuration information included in the message m1 and starts a timer $T_{handshake}$. Here, it is important to note that the node 10 does not accept the received information, before the authentication process between the segment controller 60 and the node 10 has been successfully completed. For completing the authentication handshake, the node 10 generates a handshake key $K_{handshake}$, e.g. using the
15 following expression:

$$K_{handshake} = MAC (K_{node_session} \parallel K_{seg_syst_sess})$$

Afterwards, the node 10 transmits a message N3 to the segment controller 60 including a message m2 encoded with the handshake key $K_{handshake}$. This message m2 may be the result of a function, e.g. of:

- 20 $MAC (Com2 \parallel Id_{service} \parallel Id_{segment} \parallel Id_{node} \parallel r_{session} \parallel r_{node}, K_{handshake})$,
wherein r_{node} is a random number generated by the node 10. After having received the message N3 from the node 10, the segment controller 60 verifies the message N3 by means of the handshake key $K_{handshake}$. Only the correct segment controller 60 can generate the handshake key $K_{handshake}$ for verifying this message, since this requires either knowledge
25 about the security key $K_{segment}$ of the segment controller 60, about the identity of the system and of the session, or knowledge of the session key $K_{seg_syst_sess}$. Moreover, the session-limited security key $K_{node_session}$ of the node 10 is needed. Therefore, by providing the security key $K_{node_session}$ to the segment controller 60 in the message N1, the service center 80 authorizes the segment controller 60 to transmit information to the corresponding node 10.
30 By these means, fake or non-trusted segment controllers are prevented from configuring network nodes 10.

If the verification of the message N3 is positive, the segment controller 60 will reply with a message N4 including a message m3, which is also protected with the handshake key $K_{handshake}$. The message m3 may for instance relate to the result of the following function:

HMAC (Com3 || Id_{node} || Id_{segment} || Id_{service} || r_{node} || r_{segment} || r_{session}, K_{handshake}),

wherein r_{segment} corresponds to a random number generated by the segment controller 60.

When receiving the message N4, the node 10 proceeds to the verification thereof using the handshake key K_{handshake}. If the verification is successful, the authentication of the segment

5 controller 60 to the node 10 is successfully completed. Therefore, if the message N4 is received at time T_{handshake} of the timer within a time period ΔT_{conf_node}, i.e. T_{handshake} < ΔT_{conf_node}, the node 10 accepts the information, which was included in the message m1. The time period ΔT_{conf_node} corresponds to the time interval between receiving the messages N2 and N4 at the node 10. Therefore, the time period ΔT_{conf_node} serves as a threshold time
10 defining a maximum time period, within which the authentication has to be completed. After accepting the information included in the message m1, the node 10 allows changes in its configuration parameters based on the configuration information of the message m1.

However, the service center 80 may include restrictions, so that some parameters can only be configured by the service center 80 itself. Examples of those parameters are the network
15 identifier or a network address. Similarly, threshold times ΔT₁ or ΔT₂ may be set at the segment controller 60, e.g. for the time between receiving and decoding the message N3 and transmitting the message N4 to the node 10 or between transmission of the message N4 and the receipt of a further message N5 from the node 10. These threshold times can be arbitrarily set and even be omitted in some embodiments.

20 After receiving the message N4 from the segment controller 60 in due time and accepting the configuration information, the node 10 generates an acknowledgement ACK protected with the security key K_{node} (or a key derived from it) of the node 10 and transmits this acknowledgement ACK as message m4, which is further encoded or protected based on the handshake key K_{handshake} and embedded in the message N5, to the segment
25 controller 60. Here, the acknowledgement ACK can include the received configuration parameters and/or exchanged messages protected by a message integrity code MIC or message authentication code MAC generated with K_{node}. For instance, the acknowledgement ACK may be based on the following expression:

MAC (m3 || K_{seg_syst_sess} || Configuration parameters, K_{node}),

30 When the segment controller 60 receives the message N5 including the message m4 with the acknowledgement ACK, the segment controller 60 verifies the message N5 using the handshake key K_{handshake} and forwards the acknowledgement ACK as message N6 to the service center 80. Hence, the verification or authenticity of the message N5 can be performed at the segment controller 60 before forwarding the acknowledgement ACK to the

service center 80. That is, the segment controller 60 can prove that the message N5 comes from the actual node 10 and not from another (counterfeited) entity.

As described above, the acknowledgement ACK includes a message integrity code MIC or the like of the message m3 concatenated with the configuration parameters, wherein the MIC is protected by the security key K_{node} of the node 10. By means of the security key K_{node} of the node 10, the service center 80 can verify the correct node 10 having received the information. Likewise, by means of the configuration result, e.g. the configuration parameters, the service center 80 can verify the successful transmission of information to the node 10 and the successful configuration. Furthermore, by including also the message m3 in the acknowledgement ACK, the service center 80 can verify that the actual segment controller 60 has transmitted the information to the node 10. At the service center 80, a further threshold time $\Delta T_{\text{conf_node}}$ may be set, defining a maximum allowed time period between transmitting the first set of messages N1 and receiving the message N6 reporting the acknowledgement of the node 10. These threshold times further increase the robustness of the network.

Fig. 5 shows a basic principle of the data transmission process according to an embodiment of the present invention. As illustrated in fig. 5, the service center 80 and the segment controller 60 have authenticated each other and established a secure communication channel (solid line). Moreover, the segment controller 60 is provided with the authorization to forward information from the service center 80 to one or more of the network nodes 10. Then, the segment controller 60 and each of the nodes 10 authenticate each other. After successful verification of the authorization of the segment controller 60, the nodes 10 accept data received from the segment controller 60 and employ the data correspondingly. Finally, the node 10 can confirm the secure receipt of data via the segment controller 60 to the service center 80, so that the service center 80 can verify that the node 10 has correctly received and used the data. Therefore, an indirect authentication process is performed between the nodes 10 and the service center 80 (dashed lines), while direct authentication is performed between the service center 80 and the segment controller 60 as well as between the segment controller 60 and the nodes 10 (solid lines). The indirect authentication is based on the transmission of data coded with the security key K_{node} from the service center 80 via the segment controller 60 to the node 10 and by the transmission of the confirmation message coded twice, i.e. with the handshake key $K_{\text{handshake}}$ associated to the segment controller 60 and the node 10 and with the security key K_{node} , which is known to the service center 80, but not to the segment controller 60. Therefore, according to this embodiment of the present invention, a security

handshake is mimicked between the service center 80 and the node 10 via an intermediate entity (the segment controller 60), wherein the intermediate entity, i.e. the segment controller 60 and the node 10 do not possess the respective security keys of each other.

In fig. 6, a control unit for a network node 10 according to an exemplary embodiment of the present invention is shown. The control unit 100 comprises an authentication unit 110, which can perform the mutual authentication process described above. The authentication unit 110 of the control unit 100 operates to verify the authentication of a received message, i.e. the identity of the transmitting entity such as the segment controller 60 and the identity of the origin of the message, i.e. the service center 80. A message will only be accepted by the node 10, after the authentication unit 110 has confirmed the authentication of the message. For instance, the authentication unit 110 can authenticate the node 10 to the segment controller 60 and vice versa. Moreover, the authentication unit 110 can verify, whether the segment controller 60 has been authorized by the service center 80. Therefore, the authentication unit 110 can indirectly verify the authenticity of the service center 80 and thus the origin of the message. The control unit 100 of the node 10 can further comprise a configuration unit 120 for adjusting operation parameters of the node 10 based on information included in the received message. In addition, a memory 130 and a transmission unit 140 can be included in the control unit 100 or in the node 10. In summary, the control unit 100 of the node 10 is adapted to perform the above-described processes, which are performed at the node 10.

In the foregoing description, the embodiments of the invention have been exemplified using the very sensitive situation, when a node 10 of a wireless network has to be configured. For this, a joining node 10 verifies that it is joining an allowed network, because it can verify the identity of the service center 80. In the same way, the backend or service center 80 can verify the identities of joining segment controller(s) 60 and network nodes 10, so that it can prevent copied nodes 10 or segment controller(s) 60 from joining. By means of the mutual authentication as well as by the secure transfer of configuration information and the like, dedicated customer security domains can be created and stealing of network credentials can be prevented. Moreover, the association to the network allows for service provisioning. For instance, the segment controller(s) 60 and network nodes 10 can be associated to the network for future billing. These aspects resemble the AAA (authentication, authorization, accounting) concept, in which after user authentication, an AAA server checks whether the user is authorized and accounts him for the consumed resources. However, except for commission or configuration processes of a network, there are many other

situations and systems, to which the present invention can be applied, e.g. a lightweight Zigbee-IP or 6LoWPAN/CoRE in which the essence of the above handshake is implemented by means of TLS/DTLS.

Hence, according to the present invention, means are provided for secure data
5 transmission to single network nodes 10 of a wireless network from a backend, e.g. from the service center 80. For this, operational keys are transferred in a secure way, so that key provisioning happens in a secure way. According to the present invention, the communication overhead can be minimized and security services can be provided suited for the respective application, while taking into account the restricted network resources of such
10 a wireless mesh network, as for example a lighting system or sensor system. Moreover, the protection against counterfeiting and undermining of the network by non-authorized nodes can be improved.

CLAIMS:

1. A system for secure data transmission to a node (10) of a network, comprising:
at least one node (10);
5 a service center (80) for providing the at least one node (10) with information ;
and
a segment controller (60) for providing the at least one node (10) with the
information;
wherein the segment controller (60) and the node (10) are capable of mutual
10 authentication; and
wherein the node (10) is further adapted to verify an authorization of the
segment controller (60) and to accept the provided information in case of successful
verification.
- 15 2. The system according to claim 1, wherein a session key is derived based on at
least one security key associated to an entity (10, 60, 80) involved in the mutual
authentication.
3. The system according to claim 2, wherein the service center (80) is configured
20 to inform the segment controller (60) about a session-limited security key of the node (10) for
generating the session key.
4. The system according to any one of the preceding claims, wherein the service
center (80) knows about security keys of the segment controller (60) and of the node (10)
25 and/or wherein the segment controller (60) and/or the node (10) know about its respective
security key.
5. The system according to any one of the preceding claims, wherein the service
center (80) is adapted to activate the segment controller (60) as controlling device of at least
30 some of the nodes (10).
6. The system according to any one of the preceding claims, wherein the service
center (80) is configured to distribute the information for the node (10) to the segment
controller (60) after mutual authentication between the service center (80) and the segment

controller (60) and/or wherein the segment controller (60) is configured to redistribute the information of the service center (80) to the node (10) after mutual authentication between the segment controller (60) and the node (10).

5 7. The system according to any one of the preceding claims, wherein the node (10) is adapted to send a double-coded confirmation message for the service center (80) to the segment controller (60).

8. The system according to any one of the preceding claims, wherein at least one
10 threshold time is set at the node (10) and/or at the segment controller (60) and/or at the service center (80) for defining a maximum time period allowed between two predefined messages.

9. The system according to any one of the preceding claims, wherein the node
15 (10) is configured to accept configuration information during a configuration phase.

10. The system according to any one of the preceding claims,
 wherein the service center (80) is configured to send messages for the node
(10) to the segment controller (60) encoded based on a security key associated to the node
20 (10) and on a security key associated to communication between the service center (80) and the segment controller (60); and/or

 wherein the node (10) is configured to send messages for the service center
(80) to the segment controller (60) encoded based on a security key associated to the node
(10) and on a security key associated to communication between the segment controller (60)
25 and the node (10).

11. The system according to any one of the preceding claims, wherein the segment
controller (60) is configured to provide the node (10) with information before the mutual
authentication is completed and/or wherein the node (10) is configured to accept the
30 information provided by the segment controller (60) after successful authentication and verification of the authorization of the segment controller (60).

12. The system according to any one of the preceding claims, wherein messages
between the segment controller (60) and the service center (80) are transmitted in batches.

13. The system according to any one of the preceding claims, wherein the node (10) is a luminaire node (10) of a lighting system.
- 5 14. A control unit (100) for secure data transmission to a node (10) of a network, comprising:
an authentication unit (110) for mutual authentication of the node (10) and a segment controller (60) and for verifying an authorization of the segment controller (60);
wherein information provided from a service center (80) via the segment
10 controller (60) is accepted in case of successful verification.
15. A method for secure data transmission to nodes (10) of a network, comprising the steps of:
mutual authentication of a node (10) and a segment controller (60);
15 verification of an authorization of the segment controller (60) by the node (10); and
accepting at the node (10) information provided from a service center (80) via the segment controller (60) in case of successful verification.

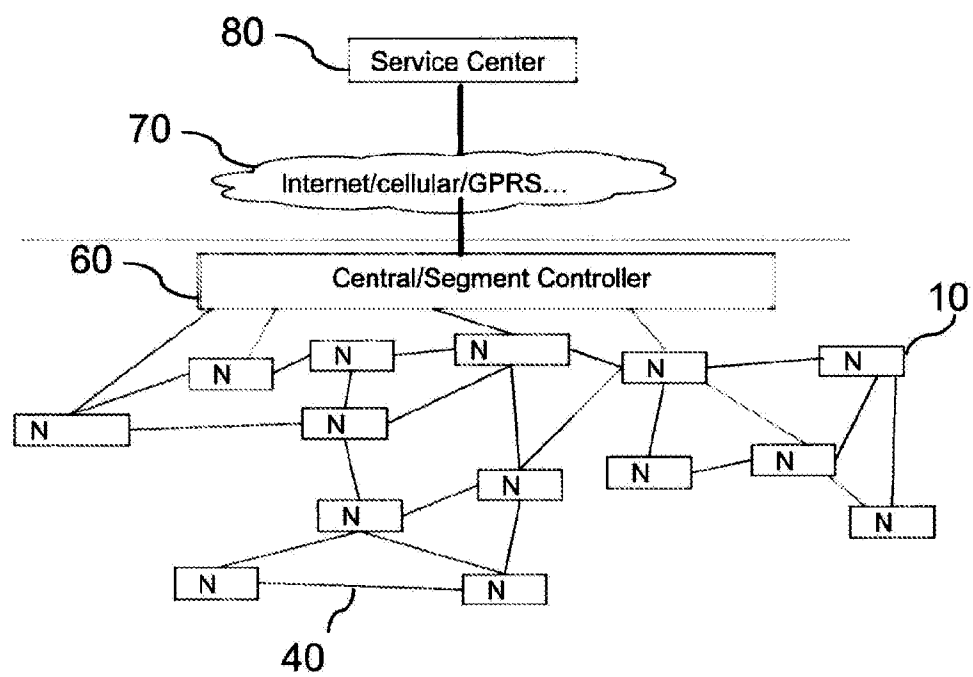


Fig. 1

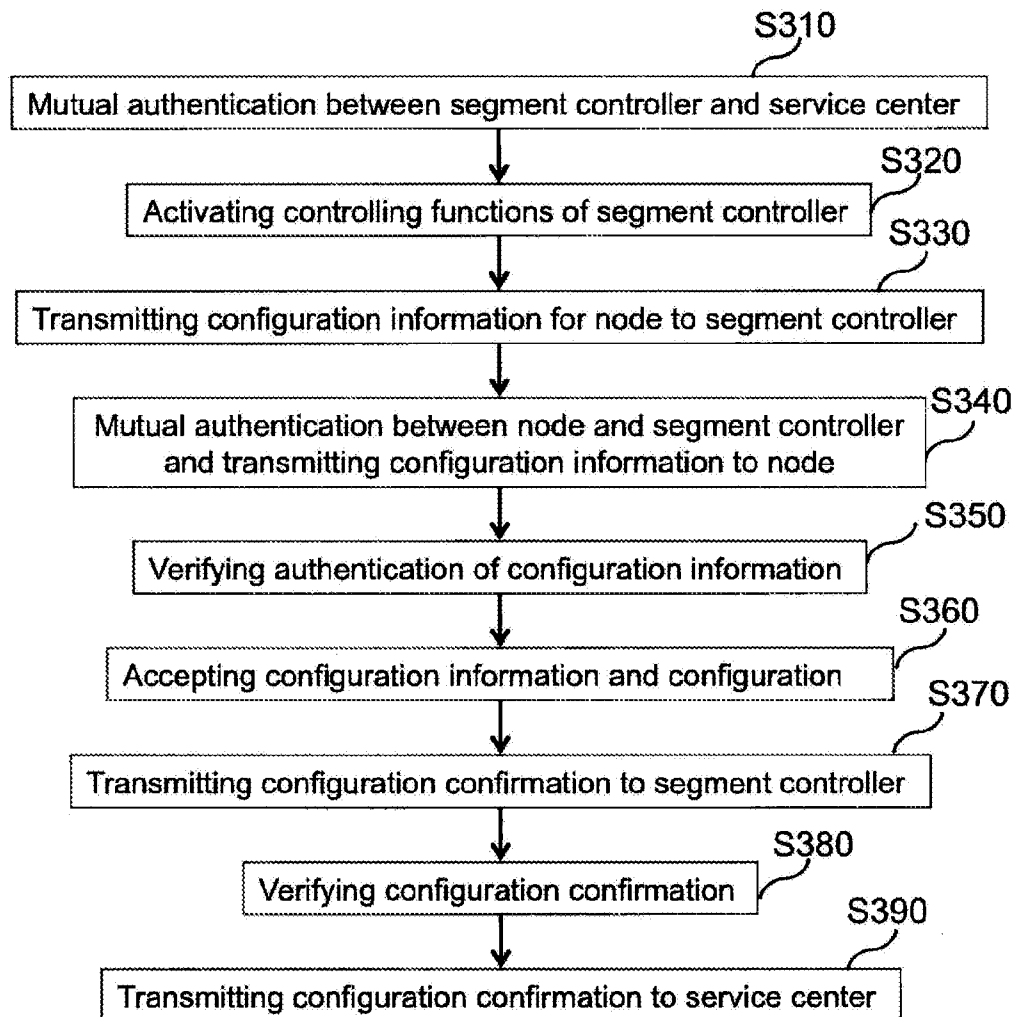


Fig. 2

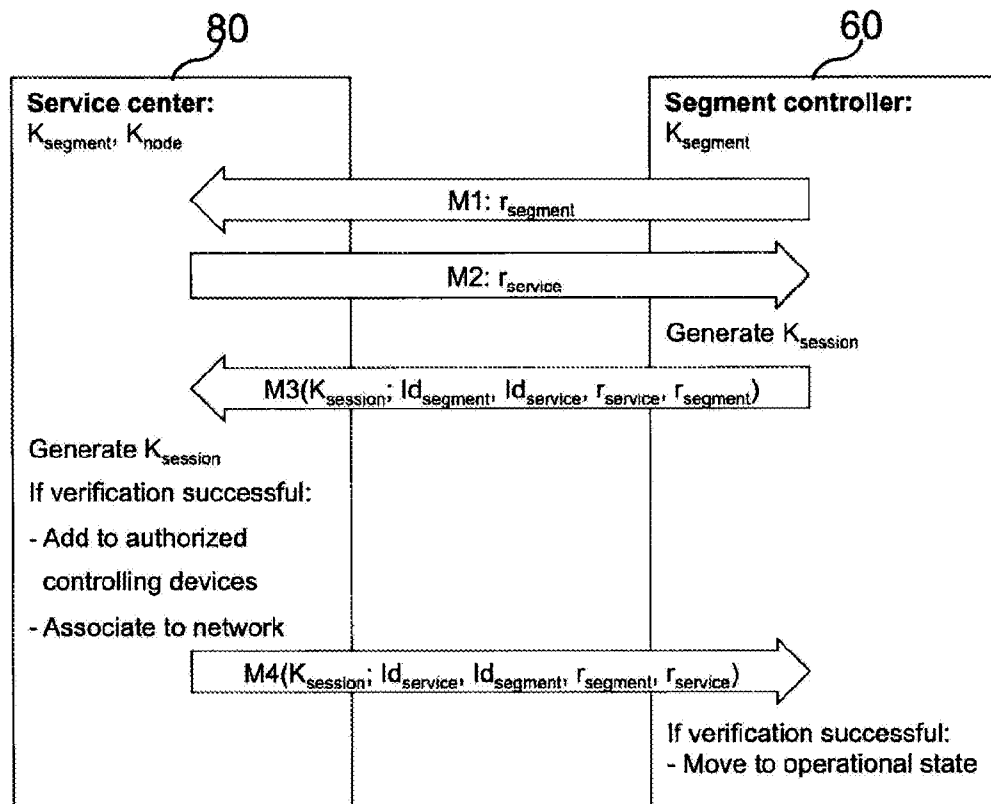


Fig. 3

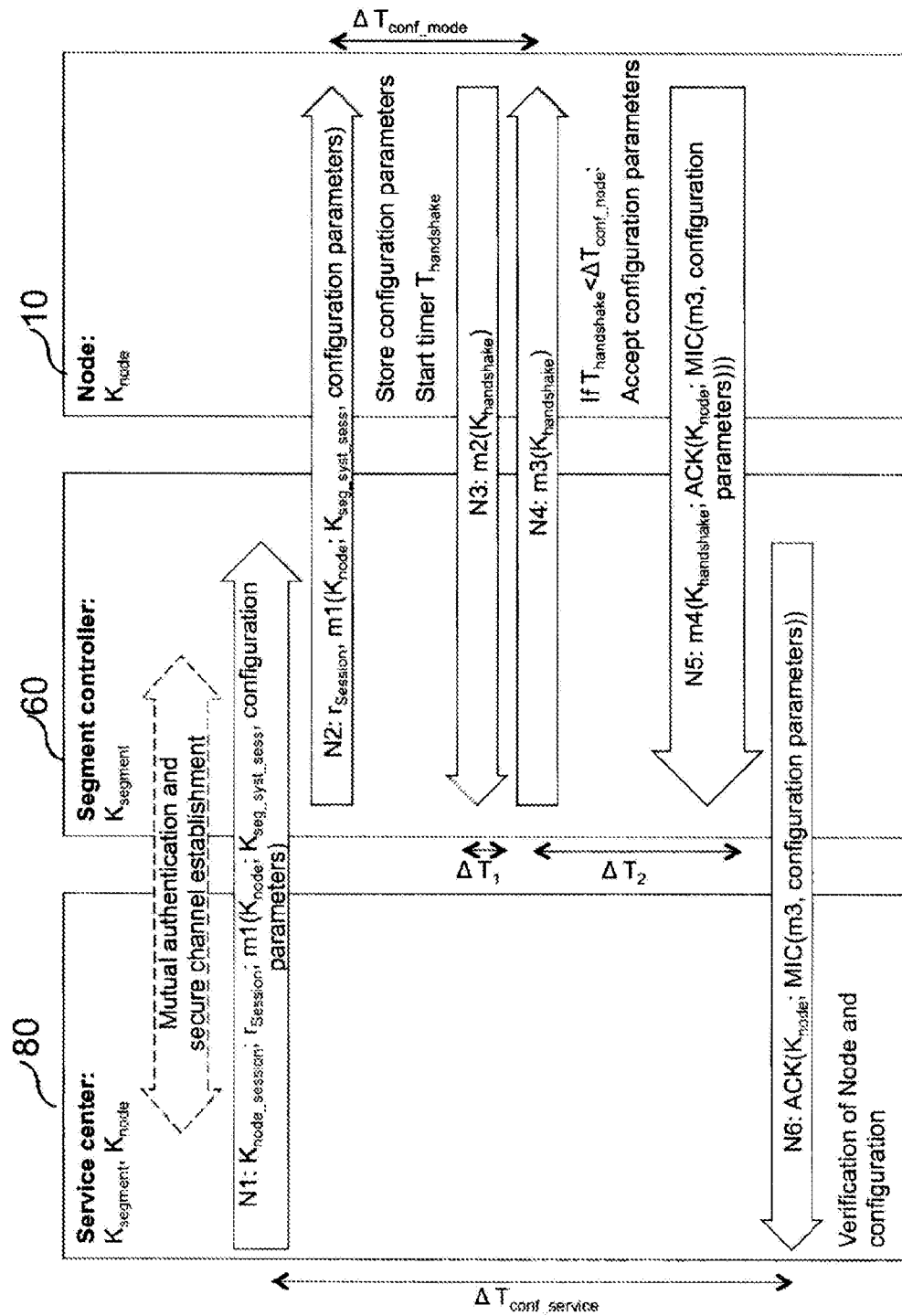


Fig. 4

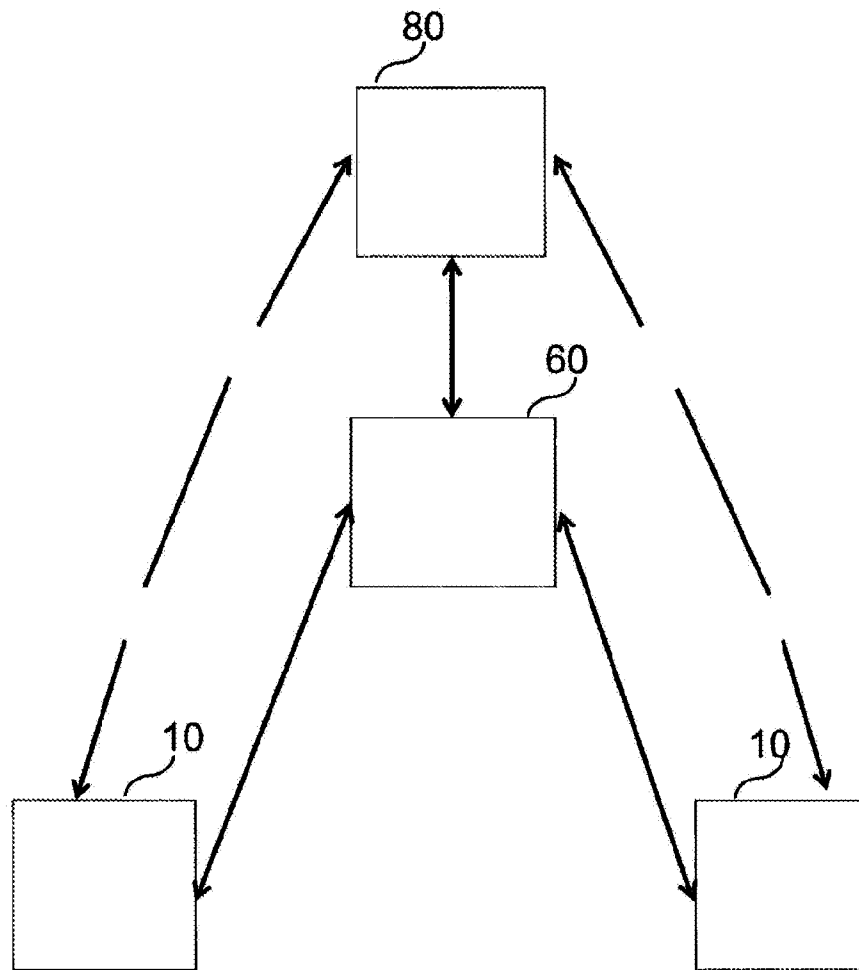


Fig. 5

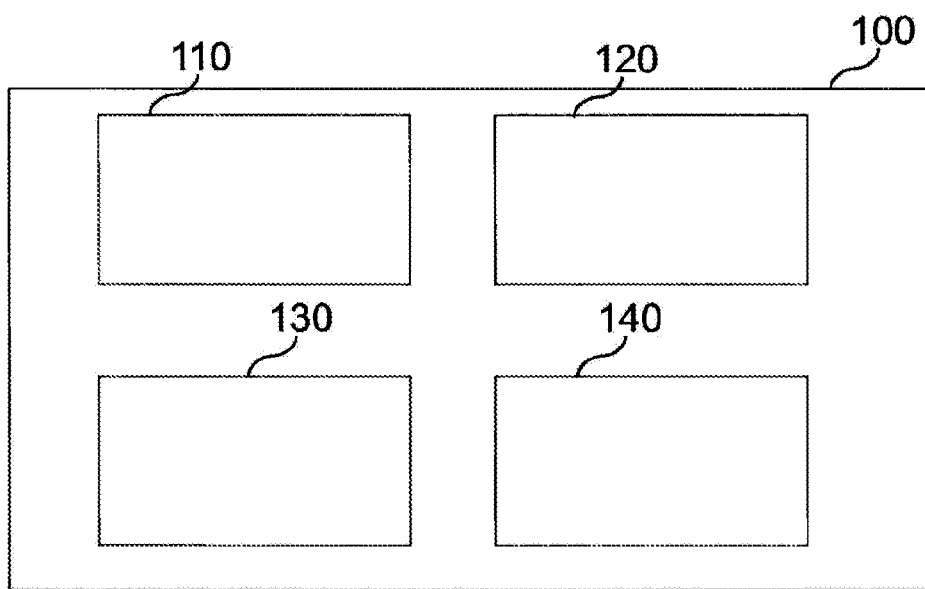


Fig. 6

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/052867

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/08 H04L9/32

ADD.

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

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Information technology - Open Systems Interconnection - Systems management overview; X.701 (08/97)", ITU-T STANDARD, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA ; CH, no. X.701 (08/97), 9 August 1997 (1997-08-09), pages 1-35, XP017462769, [retrieved on 2001-08-15] section 3.6 section 5; figure 1 ----- - / - -	1-15

☒ 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 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

12 November 2012

Date of mailing of the international search report

19/11/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Manet, Pascal

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/052867

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	"Management framework for Open Systems Interconnection (OSI) for CCITT applications; X.700 (09/92)", ITU-T STANDARD IN FORCE (I), INTERNATIONAL TELECOMMUNICATION UNION, GENEVA, CH, no. X.700 (09/92), 10 September 1992 (1992-09-10), XP017404120, section 5.5.6 -----	
T	"Security architecture for Open Systems Interconnection for CCITT applications; X.800 (03/91)", ITU-T STANDARD, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA ; CH, no. X.800 (03/91), 22 March 1991 (1991-03-22), pages 1-48, XP017462866, [retrieved on 2001-08-15] table 1 section 5.2.1.1 -----	