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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2012 (28.06.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/085744 A2

(51) International Patent Classification:
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/IB2011/055587

(22) International Filing Date:
9 December 2011 (09.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10196394.0 22 December 2010 (22.12.2010) 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)*: **GÖRGEN, Daniel, Martin** [DE/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). **GARCIA MORCHON, Oscar** [ES/DE]; 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). **ESPINA PEREZ, Javier** [ES/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).

(74) Agents: **VAN EEUWIJK, Alexander, Henricus, Walterus** et al.; High Tech Campus 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, 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, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, 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))*

[Continued on next page]

(54) **Title**: DEVICE, SYSTEM AND METHOD FOR HANDLING ALARM MESSAGE STORMS IN A COMMUNICATIONS NETWORK

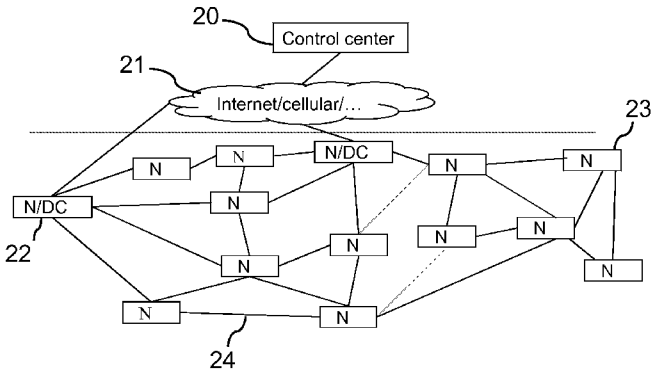

Fig. 2

(57) **Abstract**: For improving handling of alarm message storms in a communications network, alarm message storm avoidance, detection and/or recovery are implemented at nodes (23) and/or at data traffic controlling nodes (3, 20, 22) of the communications network. For alarm message storm avoidance, a random time spreading of alarm message transmissions is proposed, wherein the random time spreading of alarm message transmissions can be based on the current context and/or node state. For alarm message storm detection, it is proposed to monitor the alarm message inflow frequency to trigger a recovery process, wherein the monitoring can be performed with regard to different alarm types, parts of the network and/or time periods locally and/or centrally. The alarm message storm recovery or processing, respectively, is implemented by suppressing the amount of alarm messages to be transmitted. The alarm message storm recovery or processing can be implemented in a centralized and/or in a distributed way.

WO 2012/085744 A2

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

Device, system and method for handling alarm message storms in a communications network

FIELD OF THE INVENTION

The invention relates to handling alarm message storms in a communications network. Particularly, the invention relates to devices and methods for handling alarm message storms in a communications network, to nodes of the communications network comprising the devices and to a system comprising at least one of the nodes.

BACKGROUND

Remote management of devices or systems, also referred to as telemanagement, is receiving increased interest in the world. Remote management or telemanagement can be utilized in a plurality of areas like building automation, monitoring applications, sensor and sensor-actuator systems, medical applications, automotive techniques, automation etc. and is well known. In following, the present invention will be discussed with regard to an outdoor lighting system as an example for a system, where the remote management or telemanagement can be employed. However, it has to be pointed out, that the present invention can be used also with regard to further appropriate applications.

Recently, the remote management or telemanagement of outdoor luminaires or outdoor lighting systems respectively has received an increased interest. Thus, for example, utilization of the telemanagement enables use of different dimming patterns, such as function of time, weather conditions and season, allowing more energy efficient use of outdoor lighting systems. By use of telemanagement in an outdoor lighting system, remotely monitoring power usage and/or detecting, predicting luminaire failures, for example, can be realized, which allow determining the most suitable time for replacing luminaires, repairing luminaires and/or adjusting or controlling the operation of the luminaires.

An important application in telemanagement networks for outdoor lighting, is the communication of alarms, detected on outdoor luminaires or luminaire nodes respectively, to a control center, adapted for controlling the luminaire nodes, via collector or controller nodes, adapted for enabling and managing communications between the luminaire nodes and the control center. In the present application the terms “controller node” and “collector node” have the same meaning and refer to nodes adapted for enabling and managing communications between the luminaire nodes and the control center. The terms “luminaire node” or “node” refer to nodes, which are configured to perform applications and

functionality of the communications system or of the telemanagement network, respectively, e.g. the lighting functionality. The term "control center" refers to a central control node of the communications system of the telemanagement network, respectively, which can be a system or a device and is configured for controlling, managing and configuring the (luminaire) nodes and the collector nodes. The term "alarm" or "alarm message" respectively refers to messages, which are generated by at least one (luminaire) node if the at least one node detects that a sudden change or event in a device, system or network occurred, for example, failure, interference or other device-, system- or network-damaging, -changing or -influencing event, that has to be signaled or reported to the control center by transmitting a corresponding "alarm" or "alarm message" respectively. If too many luminaire nodes generate alarm messages simultaneously, a message storm can arise, that can congest the communications network, enabling the communication of alarms and comprising the luminaire and collector/controller nodes. In the worst case the simultaneously generated huge amount of alarm messages can cause a full or at least partial failure of communication in the communications network. Within the scope of the present invention, the term "message storm" means communication of a high number of messages in the communications network between the luminaire nodes and the control center via the collector/controller nodes so that a message overload or congestion of the communications network can, or is likely to, occur.

Handling alarm message storms, i.e. controlling alarm message overload or congestion of the communications network, is difficult due to large-scale installations (e.g. above 200 luminaires) in lighting systems. Thus, the communications network comprising the luminaire nodes and the collector or controller nodes is a large-scale network. Scalability of such large-scale networks and of applications or processes performed in the large-scale networks is known as being problematic and limited and represents a challenging task. Thus, there is still a need for efficient, robust and scalability functionality supporting handling of alarm message storms, which further allows or at least supports self-configuration and/or self-healing of the communications network and its nodes in an alarm message storm situation.

The known solutions for implementing communications networks comprising (luminaire or further device or system) nodes and collector or controller nodes can be divided in two groups: implementation of star networks and implementation of mesh networks.

Fig. 1 shows an exemplary star network, where every (luminaire) node 13 (N) is connected via a direct connection 14 to a controller or collector node 12 (DC), wherein "N" is an abbreviation for "node" and "DC" is an abbreviation for "data collector". The

controller or collector nodes 12 (DC) and the control center 10 are connected via a connection 11, which can be, for example, internet, cellular or further communication enabling network. These star networks typically require a rooftop placed high-power/high-sensitivity base station as collector or controller nodes 12 (DC), which makes the solution cumbersome to deploy and expensive. Alternatively, the collector or controller nodes 12 (DC) can be placed at a lower location (e.g. in a luminaire with one of the nodes), what, however, severely limits the cell range, especially in areas with high-rise buildings. Hence, the number of (luminaire) nodes 13 (N) per controller node 12 (DC) in such a case will typically not extend far above 100. This means that many collector or controller nodes 12 (DC) are needed, which all require an internet uplink, typically via a third party network. Another disadvantage for these star networks is that, if a controller or collector node 12 (DC) fails, all (luminaire) nodes 13 (N) connected to the controller or collector node 12 (DC) are no longer connected.

Fig. 2 shows an exemplary mesh network, which does not have the above-outlined disadvantages of the star network. Since, the present invention is directed to communications networks having the mesh network structure, a more detailed description of mesh networks is provided below, when the present invention is described in more detail. By use of the mesh network, according to the present invention, the disadvantages of the star network are overcome.

The propagation of important events, e.g. alarms, is an important application in radio frequency (RF) telemanagement systems. For lighting systems, for example, these events can be luminaire or lamp failures, driver failures, node failures or power variations being out of the specification. While alarms will typically happen very infrequently, it can occur that multiple (luminaire) nodes produce the same alarm in the same instant. As an example, a power variation can affect a neighborhood or even the whole network in a city. When too many alarms are produced and forwarded to a controller or collector node, this can lead to alarm storms that congest the communications network.

Alarm messages are in general transmitted to one or multiple controller or collector nodes that acknowledge them. In case of congestion, many data packets and/or alarm messages are lost or arrive too late at the controller or collector node, which causes corresponding retransmissions at the (luminaire) nodes. Fast retransmissions are necessary since alarms have in many cases a high importance and should be reliably communicated towards a (back-end) control center in a very short time frame. However, in case of congestion, the need for fast retransmissions leads to a further increase of the network load

and, thus, makes the problem of congestion more complicated. As mentioned, in the worst case, the communications network can be for a longer period of time not able to deliver any message in a reasonable timeframe.

Thus, there is still a need for a solution for effectively handling alarm storms to avoid the above-outlined possibilities of interference of the communications network in case of alarm message storms occurring or being likely to occur.

WO 2009/147585 A1 discloses dealing with broadcast storms due to route discovery.

SUMMARY OF THE INVENTION

In view of the above discussed disadvantages and problems, it is an object of the present invention to provide an improved handling of alarm message storms.

The object is achieved by the features of the independent claims.

The invention is based on the idea that the handling of alarm message storms can be improved by implementing alarm message storm avoidance, detection and/or recovery and by allowing appropriate combinations of alarm message storm avoidance, detection and/or recovery. Here, for the alarm message storm avoidance, a random time spreading of alarm message transmissions is proposed, wherein the random time spreading of alarm message transmissions can be based on the current context and/or node state. For the alarm message storm detection, it is proposed to monitor the alarm message inflow frequency to trigger a recovery process, wherein the monitoring can be performed with regard to different alarm types, parts of the network and/or time periods locally and/or centrally. The alarm message storm recovery or processing respectively is implemented by suppressing the amount of alarm messages to be transmitted. The alarm message storm recovery or processing can be implemented in a centralized way, where potential upcoming alarm message storms (as detected) are suppressed by triggering a quieten period from the collector node and/or from the control center (e.g. by use of a broadcast message), and/or in a distributed way, where at (luminaire) nodes the alarm messages can be aggregated to a single alarm message or it can be decided not to transmit at least a part of the alarm messages. In line with the idea of the present invention, the handling of alarm message storms is based in general on suspending the generation, transmission, retransmission and forwarding of alarm messages (for example, depending on a given alarm type etc.) and uses a random time-spread transmission period, which is more coordinated and is more targeted to the current alarm message storm.

Thus, the present invention focuses on avoiding, detecting and/or solving alarm message storms, which is one of the main reasons for limited scalability in the corresponding systems like the (outdoor) luminaire systems, for example. As pointed out above, alarming is an important application in telemanagement systems. Messages reporting the alarms are sent by the (luminaire) nodes towards a (segment) controller or collector node and subsequently towards the control center in an uncoordinated way at the time the alarm messages are created. This lack of coordination can lead to storms when too many nodes sent alarm messages at the same instant. Particularly, this may happen, for example, for the same type of alarm due to multiple nodes detecting the same phenomenon. The present invention provides a solution to avoid alarm message storms, to early detect them, to solve them.

In one aspect of the present invention, a device is provided for handling alarm message storms in a communications network at a node of the communications network, wherein the device comprises at least one of the following: an alarm message storm avoider that is adapted to transmit an alarm message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively) by randomly delaying the transmission of the alarm message according to a type of the alarm message; an alarm message storm detector that is adapted to detect alarm message storms by monitoring a number of alarm messages transmitted by the node and/or by further nodes in the communications network (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively); and an alarm message storm processor that is adapted to suppress transmitting at least one alarm message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively) with regard to an alarm message storm. In this way, an efficient alarm message storm handling is provided, by use of which congestions of the communications network can be avoided, detected and treated effectively and promptly. First of all, attention is paid to amount of messages communicated at every (luminaire) node in the communications network. Thereby, a fine distributed alarm message storm handling with high scalability is provided in large-scale communications networks, where, as known, the scalability in general represents a challenging task. Further, by use of the alarm message storm handling of the present invention, a fast and effective local handling of alarm message storms is enabled, which in known systems requires too much time and resources for detecting and processing alarm message storms not to mention avoiding of said storms. Further, in case of an alarm message storm, a fast and effective local self-healing and self-configuration is ensured by the present invention.

According to an embodiment of the present invention, at least one of the following: a maximum delay value and a delay condition, is assigned to the type of the alarm message, wherein:

- if a corresponding delay condition is assigned to the type of the alarm message and if the corresponding delay condition is met by the node, the alarm message storm avoider is adapted to transmit the alarm message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively) by randomly delaying the transmission of the alarm message;

- if the corresponding delay condition is assigned to the type of the alarm message and if the corresponding delay condition is not met by the node, the alarm message storm avoider is adapted to transmit the alarm message at a current time;

- if a corresponding maximum delay value is assigned to the type of the alarm message, the alarm message storm avoider is adapted to perform the randomly delaying the transmission of the alarm message by determining a random transmission time by use of the maximum delay and by transmitting the alarm message at the determined random transmission time.

In this way, a more specific alarm message storm handling is enabled, according to which not only quantitative alarm message storm handling but also qualitative alarm message storm handling is enabled, since also conditions existing currently in the network are taken into account for deciding on alarm message avoiding. In this way, it is ensured that urgent alarm messages will be quickly provided to the control center, wherein for the further alarm messages the random delaying of the transmission is performed carefully by considering the current situation in the network. Thus a local alarm message storm avoiding is performed in a qualitative way – by considering the state of the node in the network and by considering the sensitivity of the network with regard to the alarm messages. Thus, for example, alarm messages having high influence to other nodes in the network, would cause quickly a plurality of further alarm messages. When assigning such alarm messages to a certain type of messages and when assigning a very low value to the maximum delay value of the certain type, the plurality of further alarm messages can be avoided or at least reduced in this way.

According to an embodiment of the present invention, the alarm message storm avoider is adapted not to transmit the alarm message, if the alarm message storm avoider has received a information indicating that at least one further node of the communications network has already transmitted at least one alarm message of the type of

the alarm message, and/or wherein the alarm message storm avoider is adapted to generate a new alarm message by aggregating at least two alarm messages being alarm messages of the alarm type. In this way, an effective suppressing of the amount of communications between the nodes in the network and saving of resources of the communications network are enabled.

According to an embodiment of the present invention, the alarm message storm detector is adapted to perform said monitoring by performing an alarm message type specific monitoring, in which for each type of alarm messages a number of messages of the corresponding type of alarm messages transmitted by the node and/or by the further nodes in the communications network (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively) is monitored. Thus, a more qualitative local alarm message storm detecting is enabled, where several criteria as used for alarm message classification can be taken into account, e.g. importance or effects of an alarm message in the network.

According to an embodiment of the present invention, if the number of alarm messages exceeds a predetermined threshold value, the alarm message detector is adapted to indicate that an alarm message storm is detected; and/or if the number of messages of the corresponding type of messages exceeds a predetermined threshold value, the alarm message detector is adapted to indicate that an alarm message storm for the corresponding type of the alarm messages is detected. In this way, an effectively controllable detecting of alarm message storms can be implemented, wherein also an easy adjusting of the sensitivity of the detecting methodology is enabled, since only the parameter of the predetermined threshold value has to be amended accordingly. Further, as for every type of messages a corresponding threshold value can be specified, a more coordinated and situation-specific determining of alarm message storm is possible.

According to an embodiment of the present invention, the alarm message detector is adapted to:

- perform said monitoring by monitoring the number of alarm messages transmitted by the node and/or by further nodes in the communications network within or independently of at least one period of time and/or with regard to or independently of at least one location, to which the number of alarm messages refer; and/or

- perform said alarm message type specific monitoring by monitoring the number of messages of the corresponding type of alarm messages transmitted by the node and/or by the further nodes in the communications network within or independently of at

least one period of time and/or with regard to or independently of at least one location, to which the number of alarm messages of the corresponding type of alarm messages refer.

In this way, the local alarm message storm detecting is performed in a more qualitative and more scalable way, wherein several conditions like message types, locations or time periods are used as qualitative characteristics and since several locations of the communications (at several time periods) may be defined as focus areas for detecting alarm message storms.

According to an embodiment of the present invention, the alarm message storm processor is adapted to perform at least one of the following:

- a centralized alarm message storm processing by receiving a quieten message comprising a quieten period and by blocking transmitting of alarm messages (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively) and/or generating of alarm messages for the quieten period; and

- a distributed alarm message storm processing by not transmitting an alarm message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively), if the alarm message storm processor has received a information indicating that at least one further node of the communications network has already transmitted the alarm message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively), or by generating a single message from a plurality of messages to be transmitted and transmitting the single message (to at least one collector node (directly or via other nodes) or to a control center via at least one collector node respectively).

Thus, a centralized alarm message storm processing is performed not only with regard to a top-level of the communications network like the level of the collector nodes or the level of the control center, but, at the same time, is broken or scaled down to the node level also. Thereby, the centralized alarm message storm processing is performed not only passively but also actively at all nodes of the communications network and is performed not only with regard to the nodes but also by the nodes of the communications network. Further, also an effective distributed alarm message processing is provided, which allows reducing the amount of alarm messages to be transmitted at every node in the communications network. Thus, a strong and effective reduction of the total amount of messages transmitted in the whole communications network is achieved by involving several levels of the communications network. Thereby, the scalability requirement is supported.

According to an embodiment of the present invention, if the quieten period refers to a predefined type of alarm messages, the alarm message storm processor is adapted to block the transmitting of alarm messages of the predefined type of alarm messages; if the alarm message storm refers to a certain type of alarm messages and the information refers to the certain type of alarm messages, the alarm message storm processor is adapted not to transmit the alarm message if the alarm message is of the certain type; and/or if the alarm message storm refers to a certain type of alarm messages, the single message is generated from a plurality of messages, which are of the certain type. In this way, a more qualitative alarm message storm processing is performed, by use of which several criteria as used for classifying alarm messages can be taken into account, e.g. information as sensitivity of the network with regard to alarm messages, which caused the alarm message storm, importance of the alarm messages etc.

According to an embodiment of the present invention, the alarm message storm processor is configured to queue the alarm messages, transmission of which is blocked, during the blocking. In this way, it is ensured that none of the alarm messages blocked will be lost after the blocking process and that the corresponding alarms will actually arrive at the control center for further solving causes of the alarms.

According to an embodiment of the present invention, if the quieten period is elapsed and if the blocking is completed, the alarm message storm processor is configured to transmit the alarm messages, transmission of which has been blocked, randomly and/or to dismiss transmitting of at least one of the alarm messages, transmission of which has been blocked, if the alarm message storm processor has received an information indicating that at least one further node of the communications network has already transmitted at least one further alarm message being similar or related to the at least one alarm message. Thereby, it is avoided that a further alarm message storm will occur after completing the blocking of transmitting and/or generating of alarm messages. Thus, a permanent release of the communications network can be achieved.

According to an embodiment of the present invention, the quieten message comprises at least one of the following: a maximum delay value and a minimum delay value, wherein the random transmitting the alarm messages, transmission of which has been blocked, is performed by use of the maximum delay value and/or the minimum delay value. In this way, a specific, the detected alarm message storm oriented and considering transmission of the previously blocked alarm messages is enabled, since a maximum and/or minimum delay values can be set with regard to heaviness of traffic, i.e. the load in the

communications network, with regard to importance of the alarm messages, and/or with regard to further transmission and/or alarm message specific factors. Thereby, a more coordinated and qualitative solving of alarm message storms is performed.

In one aspect of the present invention, a device is provided for handling alarm message storms in a communications network at a data traffic controlling node of the communications network, wherein the device comprises at least one of the following: an alarm message storm detector that is adapted to detect alarm message storms by monitoring a number of alarm messages received by the data traffic controlling node (from at least one node of the communications network); and an alarm message storm processor that is adapted to suppress transmitting at least one alarm message (from at least one node of the communications network to the data traffic controlling node (directly or via other nodes)) and/or at least one alarm related message with regard to an alarm message storm. In this way, an efficient alarm message storm handling is provided, by use of which congestions of the communications network can be avoided effectively and promptly. Here, it has to be pointed out that the data traffic controlling node can be a collector node or a control center. Thus, at least one of the following: the collector node and the control center, may have the above outlined functionalities, which are explained in more detail below. The term "alarm related message" refers to messages to be transmitted and/or received due to or with regard to alarm messages, which caused the alarm message storm, e.g. acknowledgement messages acknowledging the reception of the alarm messages at the data traffic controlling node and transmitted from the data traffic controlling node to the (luminaire) nodes of the network. By handling alarm message storms at collector nodes, the intermediate level of the communications network between the nodes and the control center is utilized. Thus, the large-scale communications network and the handling of the alarm message storms are scaled down to several areas of the communications network in an efficient way. This scaling down together with the effective area based, alarm message storm handling enable a quick reacting to alarm message storms without interfering other areas of the communications network, which do not have any alarm message storm. Further, in case of an alarm message storm, a fast and effective self-healing and self-configuration of the corresponding affected area of the communications network is ensured by the present invention.

According to an embodiment of the present invention, the alarm message storm detector is adapted to perform said monitoring by performing an alarm message type specific monitoring, in which for each type of alarm messages a number of messages of the corresponding type of alarm messages received by the data traffic controlling node (from at

least one node in the communications network) is monitored. In this way, a more qualitative alarm message storm detecting is enabled, where several criteria for classifying alarm messages can be taken into account, e.g. importance of an alarm message in the network, sensitivity of the network with regard to the alarm message etc.

According to an embodiment of the present invention, if the number of alarm messages exceeds a predetermined threshold value, the alarm message detector is adapted to indicate that an alarm message storm is detected; and/or if the number of messages of the corresponding type of messages exceeds a predetermined threshold value, the alarm message detector is adapted to indicate that an alarm message storm for the corresponding type of the alarm messages is detected. In this way, an effectively controllable detecting of alarm message storms can be implemented, wherein also an easy adjusting of the sensitivity of the alarm storm detecting methodology is enabled, since only the parameter of the predetermined threshold value has to be amended accordingly. Further, as for every type of messages a corresponding threshold value can be specified, a more coordinated and situation-specific determining of alarm message storm is possible.

According to an embodiment of the present invention, the alarm message detector is adapted to: perform said monitoring by monitoring the number of alarm messages received by the data traffic controlling node within or independently of at least one period of time and/or with regard to or independently of at least one location (in the communications network), to which the number of alarm messages refer; and/or perform said alarm message type specific monitoring by monitoring the number of messages of the corresponding type of alarm messages received by the data traffic controlling node within or independently of at least one period of time and/or with regard to or independently of at least one location, to which the number of alarm messages of the corresponding type of alarm messages refer. Thereby, the alarm message storm detecting is performed in a more qualitative and scalable way.

According to an embodiment of the present invention, if the alarm message storm is detected, the alarm message storm processor is adapted to transmit a quieten message to at least one node of the communications network comprising a quieten period for blocking transmitting of alarm messages from the at least one node of the communications network to the data traffic controlling node for the quieten period; and/or if the alarm message storm is detected and if the alarm message storm refers to a certain type of alarm messages, the alarm message storm processor is adapted to transmit an alarm message type directed quieten message to at least one node of the communications network comprising a

quieten period for blocking transmitting of alarm messages of the certain type of alarm messages from the at least one node of the communications network to the data traffic controlling node for the quieten period. In this way, only a certain area of the whole communications network actually affected by the alarm message storm is processed with regard to the detected alarm message storm. Thus, an efficient and fast alarm message storm processing can be performed. Further, also a specific or targeted alarm message storm processing is executed, since only such messages which actually caused the alarm message storm are the target of the alarm message storm processing without wasting time and resources on further types of the messages.

According to an embodiment of the present invention, if the alarm message storm is detected, the alarm message storm processor is adapted to stop transmitting of acknowledgement messages acknowledging reception of alarm messages (to at least one node of the communications network) for the quieten period indicated in the quieten message; and/or if the alarm message storm is detected and if the alarm message storm refers to the certain type of alarm messages, the alarm message storm processor is adapted to stop transmitting of acknowledgement messages acknowledging reception of alarm messages of the certain type (to at least one node of the communications network) for the quieten period indicated in the alarm message type directed quieten message. In this way a further release of the communications network during the detected alarm message storm is achieved.

According to one embodiment of the present invention, the quieten message comprises at least one of the following: a maximum delay value; and a minimum delay value. In this way, a unified processing or suppressing of the alarm message storm in the corresponding area of the communications network is enabled. Further, a detected alarm message storm oriented and considering transmission of the previously blocked alarm messages is enabled, since a maximum and/or minimum delay values can be set with regard to heaviness of traffic, i.e. the load in the communications network, with regard to importance of the alarm messages, and/or with regard to further transmission and/or alarm message specific factors. Thereby, a more coordinated and qualitative solving of alarm message storms is performed.

In one aspect of the present invention, a (luminaire or other entity, device or system) node of a communications network is provided, said node comprising a device for handling alarm message storms in a communications network at the node of the communications network, said device corresponding to the above-outlined and below in more detail explained device of the (luminaire) node.

In one aspect of the present invention, a method for handling alarm message storms in a communications network at a (luminaire or other entity, device or system) node of a communications network is provided, wherein the method comprises steps relating to corresponding operations of the node or of said device of the node configured for said handling, said operations being outlined above and described in more detail below. Particularly, the method comprises at least one of the following: avoiding alarm message storms by transmitting an alarm message by randomly delaying the transmission of the alarm message according to a type of the alarm message; detecting alarm message storms by monitoring a number of alarm messages transmitted by the node and/or by further nodes in the communications network; and processing an alarm message storm by suppressing transmitting at least one alarm message with regard to the alarm message storm.

In one aspect of the present invention, a data traffic controlling node of a communications network is provided, said data traffic controlling node comprising a device for handling alarm message storms in a communications network at the data traffic controlling node of the communications network, wherein the device corresponds to the above-outlined and below in more detail explained device of the data traffic controlling node.

In one aspect of the present invention, a method for handling alarm message storms in a communications network at a data traffic controlling node of a communications network is provided, wherein the method comprises steps relating to corresponding operations of the data traffic controlling node or of said device of the data traffic controlling node configured for said handling, said operations being outlined above and described in more detail below. Particularly, the method comprises at least one of the following: detecting an alarm message storm by monitoring a number of alarm messages received by the data traffic controlling node; and processing an alarm message storm with regard to the alarm message storm by suppressing transmitting at least one alarm message and/or at least one alarm related message.

In one aspect of the present invention, a system is provided, which comprises at least one (luminaire or other entity, device or system) node of a communications network, said node being configured as outlined above and explained in more detail below, and at least one data traffic controlling node of a communications network, said data traffic controlling node being configured as outlined above and explained in more detail below. According to an embodiment of the present invention, the system is an outdoor luminaire system or outdoor lighting system, respectively.

In one aspect of the present invention, a communications network is provided, which comprises at least one (luminaire or other entity, device or system) node configured as outlined above and explained in more detail below and at least one data traffic controlling node configured as outlined above and explained in more detail below. According to an embodiment of the present invention, the communications network is a outdoor luminaire communications network or outdoor lighting communications network, respectively.

According to an embodiment of the present invention, the (luminaire or other entity, device or system) node has at least one of the following properties: the node is adapted to transmit alarm messages to one control center (via at least one collector node), i.e. to data traffic controlling nodes in general, and to receive information or data from the control center; the node has limited processing capabilities; the node is a stationary node; the node has a position, which is fixed and known in the communications network; the node transmits alarm messages and/or data messages of limited data rate. According to a further embodiment of the present invention, the communications network is a mesh network. According to another embodiment of the present embodiment, the communications network is a large-scale network. By use of the above outlined structure of the communications network and by implementing nodes of the communications network with said properties, a robust, efficient and scalable operating of the communications network and its nodes is enabled, particularly, a robust, efficient and scalable handling of alarm message storms and transmitting of data, information, (alarm) messages.

Thus, the present invention provides an improved handling of alarm message storms in a communications network, which allows a well and flexible scalability of the communications network, which is robust, fast, effective and resource saving, which takes into consideration qualitative information like importance of alarms in the communications network, locations and/or times of alarms, for example, which allows a fast and effective self-healing and self-configuration of the communications network and which enables a handling of alarm message storms that is coordinated with conditions and states in the communications network.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

Fig. 1 illustrates a communications network implemented as a star network;

Fig. 2 illustrates an exemplary communications network, with regard to which the present invention can be implemented;

Fig. 3 illustrates an arrangement of a (luminaire) node and of a data traffic controlling node according to an embodiment of the present invention;

Fig. 4 illustrates steps performed with regard to alarm message storm avoiding at a (luminaire) node according to an embodiment of the present invention;

Fig. 5 illustrates steps performed with regard to alarm message storm detecting at a (luminaire) node according to an embodiment of the present invention;

Fig. 6 illustrates steps performed with regard to alarm message storm detecting at a data traffic controlling node according to an embodiment of the present invention;

Fig. 7 illustrates steps performed with regard to alarm message storm solving or processing respectively at a data traffic controlling node according to an embodiment of the present invention;

Fig. 8 illustrates steps performed with regard to alarm message storm solving or processing respectively at a (luminaire) node according to an embodiment of the present invention;

Fig. 9 illustrates alarm message storm processing at a collector node according to an embodiment of the present invention;

Fig. 10 illustrates architecture of a (luminaire) node according to an embodiment of the present invention;

Fig. 11 illustrates architecture of a (luminaire) node according to a further embodiment of the present invention; and

Fig. 12 illustrates operations performed with regard to distributed alarm message storm processing or solving at a (luminaire) node according to an embodiment of the present invention.

DETAILED DESCRIPTION

Fig. 2 illustrates an exemplary communications network, with regard to which the present invention can be implemented. According to the embodiment of Fig. 2, the communications network is a mesh network comprising a plurality of nodes 23 (N) and a

plurality of collector nodes 22 (N/DC), all of them connected to each other via wireless connections 24. Since the present invention is explained by use of the example of (outdoor) lighting systems, the nodes 23 (N) correspond the luminaire nodes in the lighting system. However, in following also the general term "node" instead of the term "luminaire node" is used to indicate that the present invention is applicable correspondingly also to further areas like building automation, monitoring applications, sensor and sensor-actuator systems, medical applications, automotive techniques, automation etc. and is not limited to (outdoor) lighting systems only. Thus the nodes 23 (N) may be also further device, entity or system nodes. Among the nodes 23 (N) and the collector nodes 22 (N/DC), wireless connection paths can be provided, each of the paths comprising a plurality of wireless connections 24. The nodes 23 (N) are configured to transmit information or data to other nodes 23 (N), 22 (N/DC), wherein the collector nodes 22 (N/DC) represent a specific kind of nodes of the communications network – nodes, which are adapted to receive the information or data from nodes 23 (N) and to transmit this information to a control center 20, which can be a device or system being adapted to control the communications network. Thus, the collector nodes 22 (N/DC) may operate in the manner of gateways between the nodes 23 (N) and the control center (20), which receive, collect the data or information from the nodes 23 (N) and forward the corresponding data or information to the control center (20). Further, the communication can be performed also in the opposite way, where the control center (20) transmits data or information to the nodes 23 (N) via the collector nodes 22 (N/DC), preferably, for controlling the nodes 23 (N). The transmitting of data or information between the nodes 23 (N) and the collector nodes 22 (N/DC) can be performed, for example, via single-hop or multi-hop transmissions. The transmitting of data or information between the control center (20) and the collector nodes 22 (N/DC) can be performed, for example, via a connection 21. The connection 21 can be, for example, a connection via an internet, mobile communications or cellular network, a radio system or other wired or wireless data transmission system. The wireless communication among the nodes 23 (N) and the collector nodes 22 (N/DC) can be constituted, for example, by RF transmissions via the wireless connections 24 or the wireless paths, respectively.

In comparison to the star network shown exemplary in Fig. 1, the present mesh network does not base on direct communication between each of the collector nodes 22 (N/DC) and the corresponding nodes 23 (N) associated to the corresponding collector node 22 (N/DC). The communication is performed by forwarding or transmitting information or data between the nodes 23 (N) and the collector nodes 22 (N/DC) via multi-hop

communications. This means that the collector nodes 22 (N/DC) can be installed flexibly with the nodes 23 (N). Further, the communications network, with regard to which the present invention is implemented, as shown exemplary in Fig. 2, meets also robustness requirements, since, if one of the collector nodes 22 (N/DC) fails, i.e., cannot perform its functions properly, the corresponding information, data or messages respectively can be routed to at least one another collector node 22 (N/DC) in the communications network. Thus, the communications network, with regard to which the present invention is implemented and which is shown exemplary in Fig. 2, has advantages with regard to deployment and robustness.

In general, mesh networks can be divided in two groups: a flooding-based mesh and a routing-based mesh, explained shortly in more detail in the following.

The flooding-based mesh is a mesh network, in which all message are forwarded by all nodes in the network. The destination node decodes the message. The advantage of this technique is that it is extremely simple: a node does not have to decide to whom to forward a message, data or information respectively, it just broadcasts it. Further, the flooding-based mesh is typically quite robust due to the large number of messages, data or information respectively. The disadvantage of the flooding-based mesh appears in large networks (say typically > a few 100), since then the overhead due to forwarding of messages, data or information respectively starts impacting the overall data rate. This means that collisions of information, data or messages respectively start to appear, such that the overall performance may be reduced.

The routing-based mesh can be classified in general in two types: a routing-based mesh having a proactive scheme and a routing-based mesh having a reactive scheme.

Proactive schemes keep all needed network paths up-to-date, e.g., by transmitting regular beacon messages to neighbors to discover efficient routing paths. To store the communications paths, every of the nodes (corresponding to nodes 23 (N) and collector nodes 22 (N/DC) of Fig. 2) may utilize a routing table. The main advantage of this type of the mesh network is the efficiency in data, information or message transmission. The main disadvantage is the scalability, since the proactive update of the routing table consumes a large part of network resources in large networks. Moreover, in large networks, large (of full) routing tables might be required in every node. Also, in the startup of the network, long time (and costly use of resources) is required to build up the routing tables.

Reactive schemes avoid the permanent overhead and large routing tables by discovering routes on demand. They use flooding to discover communications paths and

cache active routes on nodes (corresponding to nodes 23 (N) and collector nodes 22 (N/DC) of Fig. 2). When routes are used scarcely for single messages, as in the telemanagement application, flooding information, data or messages respectively instead of performing a route discovery might be performed to make the communication more efficient. If routes are kept long enough to avoid most route discovery, reactive schemes degenerate to proactive schemes with all of the advantages and disadvantages of the proactive schemes.

Thus, the main problem of the current types of mesh networks as outlined above with regard to the flooding-based mesh and the routing based mesh is the scalability.

According to the present embodiment, a communications network is utilized, which combines the positive properties of flooding- and routing-based mesh solutions, while achieving the required level of scalability. Thus, by use of the communications network as implemented according to the present embodiment, the advantages of the flooding- and routing-based mesh solutions are achieved and the scalability problem is solved.

For this, according to the present embodiment, the communications network has at least one of the following properties:

- The communications network utilizes a (very) asymmetric communication, i.e., most of the data, information or message traffic is generated by nodes 23 (N) reporting, for example, their state and power usage to the control center 20 via collector nodes 22 (N/DC). The traffic could be, for example, several Kbytes per Node 23 (N) per day. Thus, the traffic comprises a N-to-1 traffic, which can be realized by unicasts, for example. The traffic in the other direction – from the control center 20 to nodes 23 (N) – consists basically of control commands or control related data transmitted from the control center 20 via collector nodes 22 (N/DC) to the different nodes 23 (N). Thus, the traffic in the other direction comprises 1-to-1 and 1-to-N traffic, which can be realized in unicast, multicast or broadcast mode, for example.
- The number of nodes 23 (N) is extremely high compared to known wireless mesh networks, which often have less than 200 nodes.
- The nodes 23 (N) have limited processing capabilities. When considering a lighting system, for example, due to cost considerations, the processing and memory resources in the luminaire nodes will be limited.
- The nodes 23 (N) are stationary, i.e., they are fixed in their position, immobile, motionless, static, or at rest. Thus, compared to other ad hoc mesh networks, the communications network utilized according to the present embodiment of the invention is quite stationary, i.e., the nodes 23 (N) do not move, unlike the nodes in common

communications networks. Consequently, network changes will arise in the communications network mainly due to a changing environment, e.g., due to traffic. Further, all nodes may be connected to mains power.

- Positions of nodes 23 (N) are known, i.e., knowledge about the physical positions of the nodes (e.g. GPS coordinates) is known and accessible in the system, which might be required on application level.
- The required data rate is limited. That means that the considered application usually will not require a high data rate. However, there could be some scenarios, where a low response time is needed with regard to some certain types of messages (e.g. switching lighting nodes of a section, where a traffic accident happened, to a full power level after the traffic accident).

Fig. 3 illustrates an arrangement of a (luminaire) node 23 and of a data traffic controlling node 3 according to an embodiment of the present invention. As mentioned above, the data traffic controlling node 3 refers to collector nodes 23 and to the control center 20. Therefore, it is to understood, that the collector nodes 23 and/or control center 20 may be arranged as shown exemplary in Fig. 3 with regard to the data traffic controlling node 3. The node 23 comprises a device 33 for handling alarm message storms in a communications network like the above-discussed network provided exemplary in Fig. 2. According to the present embodiment, the device 33 of the node 23 comprises an alarm message storm avoider 331 that is adapted to transmit an alarm message by randomly delaying the transmission of an alarm message, an alarm message storm detector 332 that is adapted to detect alarm message storms by monitoring a number of alarm messages transmitted by the node 23 and/or by further nodes 23 in the communications network, and an alarm message storm processor 333 that is adapted to suppress transmitting at least one alarm message at current time with regard to an alarm message storm. Also the data traffic controlling node 3 comprises according to the present embodiment a device 32 for handling alarm message storms in the communications network, wherein the device 32 of the data traffic controlling node 3 comprises an alarm message storm detector 322 that is adapted to detect alarm message storms by monitoring a number of alarm messages received by the data traffic controlling node 3 and an alarm message storm processor 323 that is adapted to suppress transmitting at least one alarm message or at least one alarm related message at current time with regard to an alarm message storm. In following, operating of the devices 33 and 32 will be explained in more detail by referring to Fig. 4 to Fig. 12.

Fig. 4 illustrates steps performed with regard to alarm message storm avoiding at a (luminaire) node 23 according to an embodiment of the present invention. In general, the box S4 comprising the steps representing the process of alarm message storm avoiding as whole. First of all, alarm messages and/or alarm situations causing generation of alarm messages are detected S41 at (luminaire) node 23. Since in general an alarm situation causes generation of a corresponding alarm message, the step S41 is referred to as alarm message detecting, although detecting of an alarm message and/or of an alarm situation can be implemented. The step S41 can be performed, for example by an alarm message detector arranged in the node 23. For this, an alarm detection algorithm (ADA) can be arranged in the alarm message detector. The alarm messages detected should be communicated as soon as possible to the data traffic controlling node 3, so that immediate actions in response to the alarm messages can be taken by the system or by the system owner. However, not all alarms are highly delay critical, and thus, an immediate delivery is not always necessary. Under specific circumstances, it can be beneficial to randomly delay an alarm message if there is a high likelihood for other nodes 22 in the communications network reporting alarm messages of the same type. It can also be possible to aggregate alarm messages coming from a given area. The node 22 might also decide not to send an alarm message, if it has heard that other nodes 22 located in its neighborhood are transmitting or broadcasting similar alarm messages. Examples for such similar alarm messages are alarms caused by lamp breakage during switching times or power variations being out of specification.

In the corresponding system (according to the present embodiment, the (outdoor) lighting system), alarm messages are classified, for example, by: importance of the alarm messages, determined, for example, by use of a degree of heaviness of damage, interference or fault in the system indicated by an alarm message; delay sensitivity, meaning whether corresponding actions in response to an alarm message should be performed immediately or may performed at a later point of time; and likelihood of concurrency. Alarm message types classified can further depend on time, at which the corresponding alarm message has been generated, or node state, corresponding to which the alarm message has been generated. For example, switching hours have the highest likelihood of lamp breakages.

When at least one alarm message has been detected, the alarm message is checked S42 by the alarm message storm avoider 331 of the (luminaire) node 23. According to the present invention, to every alarm type a maximum delay value and a delay condition is assigned. The delay condition depends on the state of the node 23, at which the alarm message has been generated, but it can also have the entry “delay always”, if the alarm

message has a low importance, for example. Thus the alarm message storm avoider 331 checks S421 the type of the alarm message detected and the corresponding information associated to the type of the alarm message. According to the present embodiment, the corresponding information is the maximum delay value and the delay condition, wherein the present invention is not limited to this information only and wherein the information can be also a predetermined number of retransmissions, which the node 23 would perform with regard to a corresponding alarm message and by use of which the node 23 would decide whether the corresponding alarm message has been transmitted said number of times (if the number of retransmissions is larger than the predetermined number, no transmission will be performed, otherwise the alarm message will be transmitted). Additionally, the alarm message storm avoider 331 checks also whether further messages having the same type have been transmitted S422. Then, by use of the results of the checking S421, S422, the alarm message storm avoider 331 decides S43 on transmitting of the alarm message.

At first, the alarm message storm avoider 331 decides S43, whether the alarm message should be transmitted. If the alarm message storm avoider 331 has received a information indicating that also further nodes have transmitted alarm messages of the same type, the alarm message storm avoider 331 may decide not to transmit the alarm message to avoid congestions and alarm message storms in the communications network. Then, the result of the deciding S43 on transmitting is 'No' (see S44) and in step S45 the transmission of the alarm message is dismissed. According to a further embodiment, a predetermined number 'M' for further nodes can be set, wherein for all or sub-set of types of alarm messages a corresponding number M can be set and/or for (each or at least one) specific type of alarm messages a corresponding number M can be set. Then, the alarm message storm avoider 331 may decide S43 not to transmit the alarm message if M or more than M further nodes have already transmitted alarm messages of the same type.

Further, if S44 the alarm message storm avoider 331 has decided S43 to transmit the alarm message, the time of transmission is determined S46 by the alarm message storm avoider 331. If the delay condition is met, a random propagation time, that is lower than the maximum delay value of the alarm class, is determined S46 by the alarm message storm avoider 331. For this several known methods for randomly determining the time of transmitting can be applied. According to the present embodiment, the alarm message storm avoider 331 uses a uniform distribution, thus the random transmission time is determined by the following equation:

send_time=uniform(current_time, current_time + maximum_delay),

wherein 'send_time' is the determined transmission time, 'current_time' represents the current time and 'maximum_delay' is the maximum delay value assigned to the type of the alarm message and provided as a value for a time period. If the delay condition is not met at node 23, the alarm message is sent immediately, i.e. the transmission time is determined S46 as being equal the current time. Then, in step S47, the alarm message is transmitted at the determined transmission time by the node 23 or the alarm message storm avoider 331.

Further, if more than one alarm message of the same type has been detected, the alarm message storm avoider 331 can generate a new alarm message of the type by aggregating the alarm messages, i.e. the alarm messages are composed or combined to the one new message. In this case, in step S47, the new alarm message is transmitted at the determined transmission time (determined S46 with regard to the type of the alarm message).

Fig. 5 illustrates steps performed with regard to alarm message storm detecting at a (luminaire) node 23 according to an embodiment of the present invention. In general, the box S5 comprising the steps represent the process of alarm message storm avoiding as whole at the node 23. Since the alarm message storm detecting S5 can be performed at every (luminaire) node 23 in the communications network, the alarm message storm detecting S5 performed by the node 23 and shown exemplary in Fig. 5 is referred to also as distributed alarm storm detecting. To this, in step S51, the alarm message storm detector 332 of the device 33 of the node 23 keeps track of the number of all sent, overheard and/or forwarded alarm messages, i.e. of alarm messages transmitted by the node 23 and/or by other nodes 23 in the communications network. This can be done, for example, within a sliding temporal window or a further entity having a data structure appropriate for monitoring and analyzing data. If the number of alarm messages is above a given or predetermined threshold value S52, the alarm message storm detector 332 indicates S53 that an alarm message storm has been detected, otherwise S52 the monitoring S51 of the number of alarm messages is continued.

With regard to the alarm message storm detecting, it can be distinguished whether the detecting is performed at a node 23, which is forwarding alarm messages originating from at least one further node 23 in the communications network. In this case, a further criteria can be applied in addition to the threshold-criterion. Thus, an alarm message storm can be detected, when the number of alarm messages exceeds the threshold value and if the alarm messages, for which the number of alarm messages has been determined, are originated from the same area of the communications network, i.e. nodes 23, which are located in the same area and/or which are neighboring nodes. Thus, in such a case the monitoring S51 can be performed with regard to several areas or locations of the

communications network, wherein for each area or location a corresponding number of alarm messages is monitored and compared S52 with the threshold value. In this way, a scaled and location based (distributed) alarm message storm detecting can be performed. The alarm message detector 332 will indicate S53, that an alarm message storm with regard to the corresponding location of the communications network has been detected.

Further, independently of whether the node 23 performs forwarding functions, the alarm message storm detecting can be performed with regard to alarm types, wherein for each type of alarm messages a corresponding number of alarm messages is monitored S51. If for one of the types of alarm messages the corresponding number of alarm messages exceeds a predetermined threshold value S52, the alarm message detector 332 will indicate S53, that an alarm message storm with regard to the corresponding type of alarm messages has been detected.

Furthermore, the alarm message storm detecting can be performed with regard to specific or predetermined time periods, for example, for specific time periods, at which a high occurrence of alarm messages can be expected or which are critical for certain reasons and to which a special attention has to be paid, or with regard to a time period of a specified length and ending at the current time. In the latter case the alarm messages of a predetermined time period recently elapsed will be monitored S51. Thus, in this case, the monitoring S51 is performed with regard to at least one time period, wherein the number of alarm messages is determined with regard to the at least one time period and wherein, if the number of the alarm messages exceeds the predetermined threshold value, the alarm message detector 332 will indicate S53, that an alarm message storm with regard to the corresponding time period has been detected.

Additionally, it has been pointed out that also a combination of the above-outlined alarm message detecting methodologies can be used according to the present invention for detecting alarm message storms. Thus, the alarm message storms can be detected in general, with regard to types, locations or time periods, with regard to types and locations, with regard to types and time periods, with regard to locations and time periods, and with regard to types, locations and time periods. To this, additionally to the criteria of the number of alarm messages and the threshold value, also the criteria of types, locations and/or time periods will be applied in steps S51, S52, S53, as outlined above.

For handling the several criteria besides the threshold criterion, the monitoring S51 can be performed, for example, by use of a sliding window statistic on the number of transmitted alarm messages within the window, wherein also further appropriate entities

based on (data) structures appropriate for efficient monitoring and analyzing data can be used. As soon as the number of transmitted messages in the current window is above a given threshold value, the alarm message detector 332 checks the statistics for each alarm message type, each location and/or each time period. If the number of transmitted messages, meeting the criteria of message type, location or time period, is above a predetermined threshold value, which can be set for each alarm message type, each location and/or each time period differently and can be different from the general threshold value used for all alarm messages, the alarm messages, which meet the criteria, are considered as potentially stormy, i.e. as being a cause for the detected alarm message storm. Thus, the alarm message storm detecting can be performed with regard to several criteria at the same time and with several levels of detail at the same time.

Fig. 6 illustrates steps performed with regard to alarm message storm detecting at a data traffic controlling node 3 according to an embodiment of the present invention. In general, the steps performed for detecting alarm message storms at the data traffic controlling node 3 are similar to the above-outlined alarm message storm detecting steps performed at the (luminaire) node 23. The box S6 comprising the steps represents the process of alarm message detecting at the data traffic controlling node 3 as whole. Since the data traffic controlling node 3 refers to collector nodes 22 and/or the control center 20 and since, thus, the alarm message storm detecting S6 is performed at the data traffic controlling node 3 being a control node for communication between the (luminaire) nodes 23 and/or at the control center 20 controlling, managing and configuring the network, the alarm message storm detecting S6 performed by the data traffic controlling node 3 and shown exemplary in Fig. 6 is referred to also as centralized alarm storm detecting. To this, the alarm message detector 322 of the data traffic controlling node 3 monitors S61 the number of alarm messages received at the data traffic controlling node 3. If the number of alarm messages is above a given or predetermined threshold value S62, the alarm message storm detector 322 indicates S63 that an alarm message storm has been detected, otherwise S62 the monitoring S61 of the number of alarm messages is continued.

Also the alarm message storm detecting at the data traffic controlling node 3 can be performed with regard to further criteria besides the threshold criterion. The utilizing of further criteria is performed in the same way as described above with regard to alarm message storm detecting S5 at the (luminaire) node 23. Further, also at the data traffic controlling node 3, the monitoring S61 can be performed, for example, by use of a sliding window statistic on the number of the transmitted alarm messages within the window,

wherein in this case the monitoring S61 is performed in the same way as the monitoring at the (luminaire) node 23. However, it has to be pointed out, that the present invention allows also further methodologies, entities or structures to handle the several criteria for both the (luminaire) node 23 and the data traffic controlling node 3. Thus, the alarm message storm detecting S6 can be performed with regard to several criteria at the same time and with several levels of detail at the same time also at the data traffic controlling node 3. The predetermined threshold value can be set with regard to several factors, e.g., it can be set relative to the number of nodes 23 in the communications network and/or relative to the ratio between the number of nodes 23 and the number of collector nodes 22. Thus, for example, the predetermined threshold value could be set by assuming that, if a certain percentage of nodes transmits alarm messages, an alarm message storm situation can be caused, wherein the predetermined threshold value would then be set to the percentage of the number of nodes 22 or of the ratio between the number of nodes 23 and the number of collector nodes 22. Here, several ways of setting of the threshold value are possible and will be apparent to the skilled person.

Moreover, both the (luminaire) node 23 and the data traffic controlling node 3 can use the methodology of alarm message storm detecting for determining and monitoring correlations according to the above criteria. Further, based on the methodology of alarm message storm detecting, performed at the data traffic controlling node 3 or at any (luminaire) node 23, a watcher like a temporal window or further entities based on an appropriate (data) structure, for example, can be utilized for monitoring, analyzing and detecting alarm message traffic peaks, which are bigger than a given threshold value. Further, the nodes 23 and/or the data traffic controlling nodes 3 (collector nodes 22 and/or control center 20) can transmit information on a detected alarm message storm (indicating the storm and, if necessary, conditions used for detecting the alarm message storm) to the neighbor nodes 23 and/or neighbor data traffic controlling nodes 3 (neighbor collector nodes 22 and/or control center 20) such that also the neighbor nodes 23 and/or neighbor data traffic controlling nodes (neighbor collector nodes 22 and/or neighbor control center 20) can perform the alarm message storm processing with regard to the detected alarm message storm.

When an alarm storm has been detected, according to the present invention, alarm message storm processors 333, 323 or (luminaire) nodes 23 and/or data traffic controlling nodes 3 can be employed for solving and/or suppressing the alarm storm. The solving and/or suppressing of detected alarm storms are explained in following with regard to

operations, which can be performed at the data traffic controlling node 3 and at the (luminaire) node 23.

Fig. 7 illustrates steps performed with regard to alarm message storm solving or processing respectively at a data traffic controlling node 3 according to an embodiment of the present invention. In general, the box S7 comprising the steps represents the process of alarm message storm processing as whole at the data traffic controlling node 3. Since the alarm message storm processing S7 according to the present embodiment is performed at the data traffic controlling node 3, controlling the communication between the nodes 23 and the control center 20 and having, thus, a quite central rule in the communications processes, the alarm message storm processing S7 is referred to also as a centralized alarm message storm processing.

If an alarm message storm has been detected, the alarm message storm processor 323 generates S71 a quieten message. The quieten message comprises a time period referred in following to as quieten period for stopping creation, transmission, forwarding and/or retransmission of alarm messages in the communications network, particularly, by nodes 23 for the time period specified by the quieten period and, where necessary, for dropping related messages in the communications network for said time period. Then the alarm message storm processor 323 transmits S72 the quieten message to the nodes 23 of the communications network. The quieten message can be, for example, a broadcast message; by broadcasting S72 the quieten message from the alarm message storm processor a more effective informing of nodes 23 about the determined alarm message storm is possible. Further, the alarm message storm processor 323 can stop or dismiss S73 transmitting of acknowledgement or response messages to the nodes 23, which are usually transmitted by the data traffic controlling node 3 to the nodes 23 to acknowledge reception of alarm messages transmitted by the nodes 23 and which can be transmitted as unicast messages, for example. In this way, a further reduction of traffic on connections 24 of the communications network is achieved. Further, the alarm message storm processor 323 can transmit S74 to the control center 20 a notification message, which comprises information on the detected alarm message storm. The information may comprise, for example, an information about the quieten period. Additionally the alarm message storm processor 323 transmits the already received alarm messages to the control center 20. In Fig. 7, no execution order is indicated with regard to steps S72, S73 and S74, since they can be executed in an arbitrary order, in a sequential and/or parallel way or in only one of the two ways.

Further, if the alarm storm has been detected by use of additional criteria like types of the alarm messages, locations in the communications network and/or certain time periods, these additional criteria are considered also with regard to performing of the alarm message storm processing S7. Thus, in step S71, the quieten message is generated by incorporating information about the additional criteria (e.g. types of the alarm messages, locations in the communications network and/or certain time periods) to allow the nodes 23 to perform actions with regard alarm messages meeting the additional criteria and causing the alarm message storm. Thus, the quieten message can comprise additionally information about the additional criteria for alarm messages, which caused the storm. Additionally, the notification message transmitted to the control center 20 may also comprise a information about the additional criteria, by use of which the alarm message storm has been detected.

Furthermore, the quieten message can be generated S71 by incorporating a maximum delay value into the quieten message, the maximum delay value specifying a period of time, according to which the transmission of alarm messages after elapse of the quieten period can be delayed maximally to avoid occurrence of a new alarm message storm after the current alarm message storm processing S7. Additionally, also a minimum delay value can be incorporated into the quieten message during its generation S71, the minimum delay value specifying a further period of time, according to which the transmission of alarm messages after elapse of the quieten period can at least be delayed to avoid occurrence of a new alarm message storm after the current alarm message storm processing S7. Each of the delay values can be set, for example, in dependence on the number of nodes 23 in the network and/or on the number/frequency of received alarm messages, which is a measure for the severity of the alarm storm. According to the present invention, several corresponding setting methods known to the skilled person can be used.

In following, more concrete embodiments of the present invention will be presented exemplary with regard to (luminaire) nodes 23 and collector nodes 22 as representatives of the data traffic controlling nodes 3. However, it has to be pointed out that similar implementations can be performed also with regard to (luminaire) nodes 23 and control center 20 as a representative of the data traffic controlling node 3.

Fig. 8 illustrates steps performed with regard to alarm message storm solving or processing respectively at a (luminaire) node 23 according to an embodiment of the present invention. In general, the box S8 comprising the steps represents the process of alarm message storm processing as whole. The alarm message storm processing S8 can be performed by at least one of two further or sub-processing processes: the centralized

processing S81 and the distributed processing S82, which are performed independently in dependence of where the alarm message storm has been detected. If the alarm message storm has been detected at the collector node 22, the centralized alarm message processing S71 is performed at the node 23 with regard to the alarm message processing S6 of the collector node 22. Thus, the steps performed within the centralized alarm message processing S71 at node 22 are performed in response to the corresponding steps of the alarm message processing S6 at the collector node 22. The distributed processing S82, in turn, is performed if the alarm message storm has been detected by the node 23.

In the centralized processing S81, the alarm message storm processor 333 of the device 33 of the node 23 receives S811 a quieten message from a collector node 22, wherein the received quieten message corresponds to the above-outlined quieten message transmitted by the collector node 22 during the alarm message storm processing S7. Then, in response to the received quieten message, the alarm message storm processor 333 blocks or stops S812 creating, transmitting, forwarding and/or retransmitting of related messages for the quieten period specified in the quieten message. The related messages are messages, which have a relation to or are similar to alarm messages, which caused the alarm message storm. During the blocking step S812, the related alarm messages, transmission, retransmission and/or forwarding of which has been blocked, can be queued in a queue for a later transmitting, retransmitting and/or forwarding of said messages, i.e. after expiry of the quieten period. If appropriate, the node 23, i.e. the alarm message storm processor 333 can also drop already queued related messages. If the quieten period is expired, in step S813 creation, transmission, retransmission and/or forwarding of the related alarm messages is resumed by the alarm message storm processor 333. If the quieten message comprises also at least one of the following: a maximum delay value and a minimum delay value, the transmission, retransmission and/or forwarding of the related alarm messages (summarized in Fig. 8 by term “transmission”) can be performed by randomly delaying the transmission of the related messages, wherein the corresponding value as provided – the maximum delay value and/or minimum delay value – is used for the randomly delaying the transmission.

Further, if the alarm storm has been detected by use of additional criteria like types of the alarm messages, locations in the communications network and/or certain time periods and if these additional criteria have been specified in the quieten message, the alarm message storm processor 333 will perform the above blocking step S812 with regard to such related messages only, which also meet the additional criteria. Thus, for example, said

blocking S812 would be performed with regard to alarm messages having the same type and/or being related to the same locations and/or time periods.

In the distributed processing S82, if the alarm message storm has been detected at the node 23, e.g. by the alarm message storm detector 332, the alarm message storm processor 333 performs the distributed processing S82. At first, a decision with regard to transmitting of alarm messages is met S821. The steps S821 and S822 can be performed in similar way as described with regard to steps S43 and S44 of Fig. 4. If the alarm message storm processor 333 has received an information indicating that also further nodes have transmitted similar alarm messages, the alarm message storm processor 333 may decide not to transmit the alarm message to suppress the detected alarm message storm. Then, the result of the deciding S821 on transmitting is 'No' (see S822) and in step S823 the transmission of the alarm message is dismissed.

If the result of the deciding S821 on transmitting is 'Yes' (see S822), the alarm message storm processor 333, generates S824 a single alarm message from a plurality of alarm messages, which are related to alarm messages, that caused the detected alarm message storm, and which are to be transmitted or forwarded. The generating S824 of the single alarm message can be performed by aggregating the plurality alarm messages, i.e. the alarm messages are composed or combined to the single message. Further, the alarm message storm processor 333 may insert into the single message a information indicating the area of the communications network, where the alarm has been originated, to provide to the control center 20 a more detailed information about the detected alarm message storm. Subsequently the node 23 or the alarm message storm processor 333 transmits the single message to the control center 20 via a collector node 22.

Further, if the alarm storm has been detected by use of additional criteria like types of the alarm messages, locations in the communications network and/or certain time periods, the alarm message storm processor 333 will generate S824 the single message with regard to such related alarm messages only, which also meet the additional criteria. Thus, for example, the single message will be generated S825 with regard to alarm messages having the same type and/or being related to the same locations and/or time periods.

Fig. 9 illustrates alarm message storm processing at a collector node 22 according to an embodiment of the present invention by visualizing main phases of the centralized alarm storm processing or solving S7, respectively. Since the collector node 22 controls communication between a plurality of nodes 23 in the communications network and one control centre 20 and since alarm message storms are caused by communication of alarm

messages from the plurality of the nodes 23 to the control center 20 via the collector node 22, i.e. on the side of communications network, the communication between the collector node 22 and the nodes 23 is visualized in Fig. 9 in a more general way by summarizing the nodes 23 to a box 93 (Network).

During the normal operation, indicated by bar 94 (Normal behavior) in Fig. 9, the collector node 93 acknowledges every incoming alarm message Alarm T2 with an acknowledgement message ACK. According to the present embodiment, the acknowledgement message ACK can be, for example, a unicast message. After the normal behavior phase 94 (Normal Behavior), a stormy behavior phase 95 (Stormy behavior) with a plurality of transmitted alarm messages Alarm T2 occurs, which is monitored S6 by the alarm message storm detector 322 of the collector node 22. For this, the sliding window 98 (Sliding window) is used according to the present embodiment. As soon as a potential alarm storm for an alarm type, according to the present embodiment T2, (in a given location) is detected S6, the (unicast) acknowledgement message ACK for all alarm messages Alarm T2 of this type T2 (in that location) is suspended S73 and a quieten message Quieten is sent S72 to the network 93 to suppress further storming of this alarm message type T2 (coming from that location). The quieten message Quieten can be, for example, a broadcast message, by use of which it is ensured that every node 23 in the network 93 will receive the quieten message Quieten informing about the detected alarm message storm 99. According to the present embodiment, the quieten message Quieten contains the length of a quieten period 96 (Quiet period T2) and parameters for a coordinated alarm message delivery. In this way, a quieten period 96 (Quiet period T2) with a length specified by the collector node 22 is established in the network 93, in which no node 23 is allowed to create or forward alarm messages of the corresponding alarm type T2. After the quieten period 96 (Quiet period T2), the nodes 23 in network 93 deliver S813 the outstanding alarm messages of the corresponding alarm message type T2, which could not be transmitted during the quieting period 96 (Quiet period T2), by randomly selecting a delivery time from a time interval specified in the quieten message Quieten. The collector node 22 acknowledges the reception of the outstanding alarm messages by the acknowledgement messages ACK. The transmitting of the outstanding messages is indicated in Fig. 9 by the bar 97 (Time-spread alarm delivery). Here, the outstanding alarm acknowledgement messages ACK can be also transmitted also with regard to a batch of alarm messages and not only individually, i.e. with regard to each alarm message separately.

Fig. 10 illustrates the architecture of a (luminaire) node 23 according to an embodiment of the present invention, showing components of the node 23, which can be involved for centralized alarm message storm processing S81 and for creating or establishing a quieten period in the node 23. The alarm message storm processor 333 of the device 33 of the node 23 comprises a forward decider 10_1 (FD) that is adapted to check the type of each alarm message to be forwarded or transmitted; a router component 10_2 (Router) adapted to receive alarm messages and to pass each alarm message to the forward decider 10_1 (FD) before the corresponding alarm message is forwarded or transmitted to other nodes 22, 23 in the communications network; an alarm application component 10_3 (Alarm App.) adapted to block and unblock message types corresponding to alarm message types responsive for the detected alarm message storm and to drop alarm messages of a specific alarm message type, that are already scheduled for forwarding but alarm message type of which is involved in the detected alarm message storm; a queue component 10_4 (Queue) adapted to queue the alarm messages dropped by the alarm application component 10_3 (Alarm. App.), wherein the router component 10_2 (Router) is further adapted to enqueue the alarm messages, i.e. to derive the alarm messages from the queue component 10_4 (Queue) for forwarding or transmitting them to other nodes 22, 23 in the communications network. Further, according to the present embodiment, the node 23 can comprise another application component 10_5, which can communicate also during an alarm message storm situation, if necessary, and which can receive/send messages from/via the router component 10_2, and a network interface controller 10_6 (NIC), which provides alarm and other messages received from the network to the router component 10_2 (Router). According to the present embodiment, the architecture of node 23 comprises three layers: application layer, network layer and link layer, comprising the above mentioned components as shown in Fig. 10.

Fig. 11 illustrates the architecture of a (luminaire) node 23 according to a further embodiment of the present invention. According to the present embodiment, components of the node 23 involved in the distributed alarm message storm detecting and processing S82 are visualized. According to the present embodiment, the node 23 comprises an alarm detection (AD) component 11_1 adapted to detect S11_1 possible alarm situations based on information such as measured information, node status, or local radio frequency communication. If an alarm is detected, it is sent S11_2 from the alarm detection (AD) component 11_1 to an alarm sending unit 11_2 of the node 23 that will further transmit S11_3 it to the network 11_4 (NWK), i.e. to further nodes 23 and/to collector nodes 22. According to the present embodiment, the node 23 analyzes also alarm messages transmitted

around the node 23 in the communications network. Alarm forwarding unit 11_3 of the node 23 detects the alarm messages in the communications network and sends S11_5 statistics on these alarm messages to the alarm message storm detector 332 (SD). As already described above, the alarm message storm detector 332 analyzes different parameters to detect alarm message storms. Based, for example, on the type of the alarm messages, with regard to which the alarm message storm has been detected, on the location and/or on frequency, the node 23 can perform several operations with regard to the detected alarm message storm, as described above. For example, the node 23 can drop S11_7a its own alarm messages (e.g., because similar ones are already transmitted in the communications network) or aggregate S11_7b the alarm messages or drop S11_7b repeated alarm messages. The alarm detection (AD) component 11_1 transmits S11_6 information on detected alarm messages to the alarm message storm detector 332 (SD), which analyzes (amount of) the alarm messages with regard to a possible alarm message storm situation.

According to a further embodiment of the present invention, for example, each node 23 in the communications network keeps track of the alarm messages that it has heard from its neighbors or that it has forwarded. According to another embodiment, if the alarm detection component 11_1 (AD) of a node 23 triggers an alarm, but the node 23 has already heard similar alarms in its neighborhood, the alarm message storm detector 332 (SD) of the node 23 can decide not to send the alarm message (e.g., in case of alarms restricted to a given area). According to other embodiment, a router component of the node 23, corresponding to the above-outlined alarm message storm processor 333, will check the alarm type, location, and time of each forwarded alarm message. Based on this information, the router keeps track of alarm statistics and looks for correlations that enable reducing the amount of alarm-related traffic without reducing the effectivity of the system. In this case, the router component, relying on an alarm message storm detector 332 (SD), can decide not to forward alarm messages that are redundant. Alternatively, the router can decide to aggregate related alarm messages, e.g., originated in the same area.

Fig. 12 illustrates operations performed with regard to distributed alarm message storm processing or solving S82 at a (luminaire) node 23 according to an embodiment of the present invention. Particularly, Fig. 12 gives an example for handling a quieten message, transmitted by a collector node 22 to the node 23, by components of the alarm message storm processor 333 as exemplary provided in Fig. 10. At first the quieten message is received by the router component 10_2 of the alarm message storm processor 333 of the node 23 and provided to the alarm application component 10_3 of the alarm message

storm processor 333, wherein the alarm application component 10_3, according to the present embodiment, is adapted to:

- cancel all outstanding transmissions and/or retransmission of alarm messages of the alarm type indicated in the quieten message, wherein the outstanding messages are cached, i.e. queued in the interface queue component 10_4 of the alarm message storm processor 333;
- block messages of the alarm type, indicated in the quieten message, by accessing and/or transmitting a blocking message to the forward decider component 10_1 of the alarm message storm processor 333;
- optionally drop all alarm messages of the alarm type, indicated in the quieten message, from the interface queue component 10_4 of the alarm message storm processor 333;
- block any further local alarm message generation for the alarm type, indicated in the quieten message;
- set a timer based on the quieten period interval indicated in the quieten message.

If the quieten period timer expires, the forwarding and/or transmitting of alarm messages is unblocked and the node 23 or the alarm message storm processor 333 checks whether it has alarm messages of this type cached (e.g. in the interface queue component 10_4). If it does, it uses a maximum delivery delay value 'maximum_delay' indicated in the quieten message to schedule the delivery or transmission of the alarm messages. The scheduling of the alarm messages can be performed by use of several known and appropriate scheduling methods. According to the present embodiment, the following equation is used for randomly determining the transmission time 'send_time', at which an alarm message should be transmitted:

send_time=min_delay + uniform(current_time, current_time + maximum_delay)

According to the present embodiment, the value 'min_delay', indicating a minimum delay time for the transmission, ensures that all other nodes 23 have already unblocked the forwarding or transmitting too. Since normal operation of communication is reestablished after expiration of the quieten period, the alarm messages are acknowledged by acknowledgement messages (e.g. unicasts) by the collector node 22 in response to receiving the alarm messages. Here, the transmitting of the acknowledgement messages can be done also by broadcasting the acknowledgement messages to limit the traffic. The 'maximum_delay' is a critical parameter. It has to be chosen such that all potential alarm message senders 23 can communicate their alarm messages without creating an alarm message storm. If this number cannot be estimated, it can be assumed that all nodes 23 have

to send an alarm, to derive the worst-case parameters (e.g. based on the estimated number of alarms, based on number of nodes in an area of alarms etc.).

The detection of a potential alarm message storm can be communicated to the control center 20, wherein also all already received alarm messages of the alarm type, with regard to which the alarm message storm has been detected, are communicated to the control center 20. By this communication, the alarm situation is communicated early to the control center 20, so that it can perform the current control of the communications network by use of current information and based on the detected alarm message storm situation. The further details, i.e. the remaining alarm messages, are provided later when the communications network (i.e. nodes 23 and collector nodes 22) has transmitted the alarm messages after the quieten period in a coordinated way.

Additionally, it has to be noted that the quieten message, which is generated in a centralized approach by the collector node 22, can be equivalent to the signal locally triggered to a router 10_3 by the alarm message storm detector 332 and that allows the router 10_3 to detect the alarm message storm before arriving the collector node 22. Further, according to an embodiment of the present invention an alarm message storm detector of a router 10_3 can take a decision regarding the dropping or not forwarding of message for a given period of time T_D or $T_{not\text{-}forwarding}$. These times can be calculated in different ways. For instance, the first time an alarm is detected $T_{D\text{-}0}$ can take an initial time T_{Ini}. After expiration of the corresponding counter, the alarm message storm detector can check whether another storm is detected within a delta of time. In this case, the alarm message storm detector starts again dropping or forwarding messages for a new period of time $T_{D\text{-}1}$ that is a function of the last value $T_{D\text{-}0}$, for instance, $T_{D\text{-}1} = 2T_{D\text{-}0}$. In other words, the waiting time grows exponentially until the alarm message flow stops for at least a delta of time.

It is obvious that the above-described embodiments can be combined in various ways. By means of the above described alarm message storm avoiding, detecting and/or processing an effective and fast handling of alarm message storms is enabled, such that alarm message overloads and congestions of the communications network are avoided. Further, the alarm message storm avoiding, detecting and/or processing according to the present invention are provided with a high scalability in a large-scale communications network and enable an efficient and effective self-healing and self-configuration in the communications network, particularly, of nodes and collector nodes in the communications network.

CLAIMS

1. A device (33) for handling an alarm message storm in a communications network at a node (23) of the communications network, wherein the device (33) comprises at least one of the following:

- an alarm message storm avoider (331) that is adapted to transmit an alarm message by randomly delaying the transmission of the alarm message according to a type of the alarm message;
- an alarm message storm detector (332) that is adapted to detect the alarm message storm by monitoring a number of alarm messages transmitted by the node and/or by further nodes in the communications network; and
- an alarm message storm processor (333) that is adapted to suppress transmitting at least one alarm message with regard to the alarm message storm.

2. The device (33) according to claim 1, wherein at least one of the following is assigned to the type of the alarm message: a maximum delay value and a delay condition, wherein:

- if a corresponding delay condition is assigned to the type of the alarm message and if the corresponding delay condition is met by the node, the alarm message storm avoider (331) is adapted to transmit the alarm message by randomly delaying the transmission of the alarm message;
- if the corresponding delay condition is assigned to the type of the alarm message and if the corresponding delay condition is not met by the node, the alarm message storm avoider (331) is adapted to transmit the alarm message at a current time;
- if a corresponding maximum delay value is assigned to the type of the alarm message, the alarm message storm avoider (331) is adapted to perform the randomly delaying the transmission of the alarm message by determining a random transmission time by use of the maximum delay and by transmitting the alarm message at the determined random transmission time.

3. The device (33) according to any one of the preceding claims, wherein the alarm message storm avoider (331) is adapted not to transmit the alarm message, if the alarm message storm avoider (331) has received a information indicating that at least one further

node of the communications network has already transmitted at least one alarm message of the type of the alarm message, and/or wherein the alarm message storm avoider (331) is adapted to generate a new alarm message by aggregating at least two alarm messages being alarm messages of the alarm type.

4. The device (33) according to any one of the preceding claims, wherein the alarm message storm detector (332) is adapted to perform said monitoring by performing an alarm message type specific monitoring, in which for each type of alarm messages a number of messages of the corresponding type of alarm messages transmitted by the node and/or by the further nodes in the communications network is monitored.

5. The device (33) according to any one of the preceding claims, wherein:
- if the number of alarm messages exceeds a predetermined threshold value, the alarm message detector (332) is adapted to indicate that an alarm message storm is detected; and/or
- if the number of messages of the corresponding type of messages exceeds a predetermined threshold value, the alarm message detector (332) is adapted to indicate that an alarm message storm for the corresponding type of the alarm messages is detected.

6. The device (33) according to any one of the preceding claims, wherein the alarm message storm processor (333) is adapted to perform at least one of the following:
- a centralized alarm message storm processing by receiving a quieten message comprising a quieten period and by blocking transmitting and/or generating of alarm messages for the quieten period; and
- a distributed alarm message storm processing by not transmitting an alarm message, if the alarm message storm processor (333) has received a information indicating that at least one further node of the communications network has already transmitted the alarm message, or by generating a single message from a plurality of messages to be transmitted and transmitting the single message.

7. A method for handling an alarm message storm in a communications network at a node (23) of the communications network, wherein the method comprises at least one of the following:
- avoiding (S4) an alarm message storm by transmitting an alarm message by randomly delaying the transmission of the alarm message according to a type of the alarm message;

- detecting (S5) an alarm message storm by monitoring a number of alarm messages transmitted by the node and/or by further nodes in the communications network; and
- processing (S8) an alarm message storm by suppressing transmitting at least one alarm message with regard to the alarm message storm.

8. A device (32) for handling an alarm message storm in a communications network at a data traffic controlling node (3, 20, 22) of the communications network, wherein the device (32) comprises at least one of the following:
- an alarm message storm detector (322) that is adapted to detect the alarm message storm by monitoring a number of alarm messages received by the data traffic controlling node (3, 20, 22); and
- an alarm message storm processor (323) that is adapted to suppress transmitting at least one alarm message and/or at least one alarm related message with regard to the alarm message storm.

9. The device (32) according to claim 8, wherein the alarm message storm detector (322) is adapted to perform said monitoring by performing an alarm message type specific monitoring, in which for each type of alarm messages a number of messages of the corresponding type of alarm messages received by the data traffic controlling node (3, 20, 22) is monitored.

10. The device (32) according to claim 8 or 9, wherein:
- if the number of alarm messages exceeds a predetermined threshold value, the alarm message detector (322) is adapted to indicate that an alarm message storm is detected; and/or
- if the number of messages of the corresponding type of messages exceeds a predetermined threshold value, the alarm message detector (322) is adapted to indicate that an alarm message storm for the corresponding type of the alarm messages is detected.

11. The device (32) according to any one of the preceding claims 8 to 10, wherein:
- if the alarm message storm is detected, the alarm message storm processor (323) is adapted to transmit a quieten message to at least one node (23) of the communications network comprising a quieten period for blocking transmitting of alarm messages from the at least one node (23) of the communications network to the data traffic controlling node (3, 20, 22) for the quieten period; and/or

- if the alarm message storm is detected and if the alarm message storm refers to a certain type of alarm messages, the alarm message storm processor (323) is adapted to transmit an alarm message type directed quieten message to at least one node of the communications network comprising a quieten period for blocking transmitting of alarm messages of the certain type of alarm messages from the at least one node (23) of the communications network to the data traffic controlling node (3, 20, 22) for the quieten period; and/or
- if the alarm message storm is detected, the alarm message storm processor (323) is adapted to stop transmitting of acknowledgement messages acknowledging reception of alarm messages for the quieten period indicated in the quieten message; and/or
- if the alarm message storm is detected and if the alarm message storm refers to the certain type of alarm messages, the alarm message storm processor (323) is adapted to stop transmitting of acknowledgement messages acknowledging reception of alarm messages of the certain type for the quieten period indicated in the alarm message type directed quieten message.

12. A method for handling an alarm message storm in a communications network at a data traffic controlling node (3, 20, 22) of the communications network, wherein the method comprises at least one of the following:
- detecting (S6) the alarm message storm by monitoring a number of alarm messages received by the data traffic controlling node (3, 20, 22); and
- processing (S7) the alarm message storm by suppressing transmitting at least one alarm message and/or at least one alarm related message with regard to the alarm message storm.

13. A node (3, 20, 22, 23) of a communications network comprising a device (33) according to any one of claims 1 to 6 or comprising a device (32) according to any one of claims 8 to 11.

14. A system comprising at least one of following: at least one node (23) of a communications network comprising a device (33) according to any one of claims 1 to 6 and at least one data traffic controlling node (3, 20, 22) of the communications network comprising a device (32) according to any one of claims 8 to 11.

15. The system according to claim 14, wherein the system is an outdoor luminaire system.

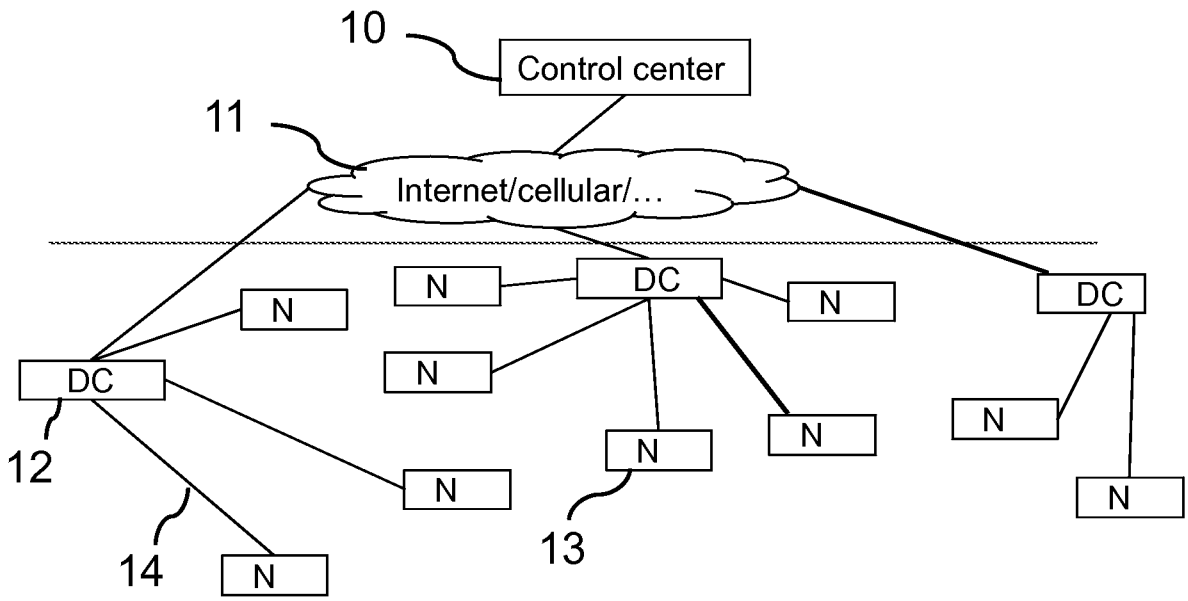
10
Control center
11
Internet/cellular/…
N
DC
N
DC
N
N
DC
N
N
12
N
N
N
N
13
14
N

Fig. 1

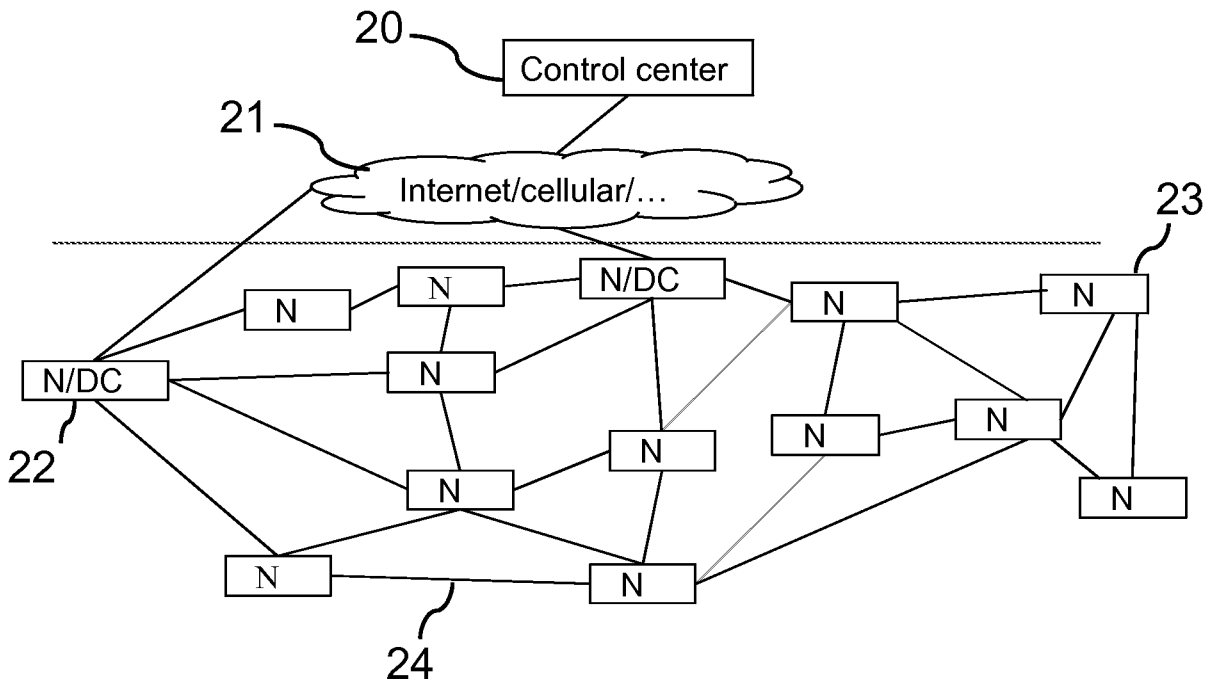
20
Control center
21
Internet/cellular/…
23
N
N
N/DC
N
N
N/DC
N
N
N
N
22
N
N
N
N
N
N
24

Fig. 2

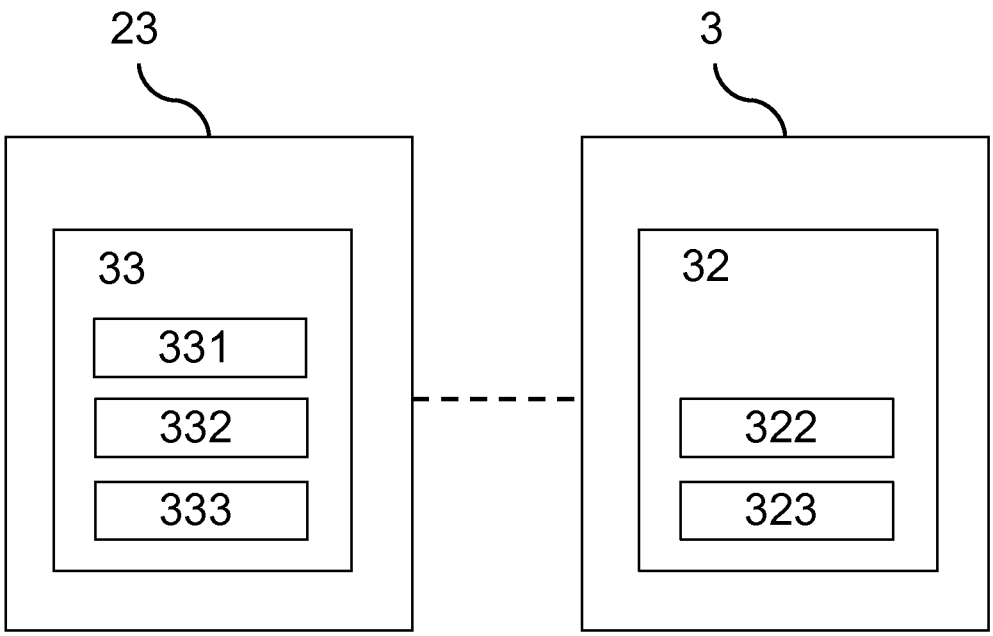

Fig. 3

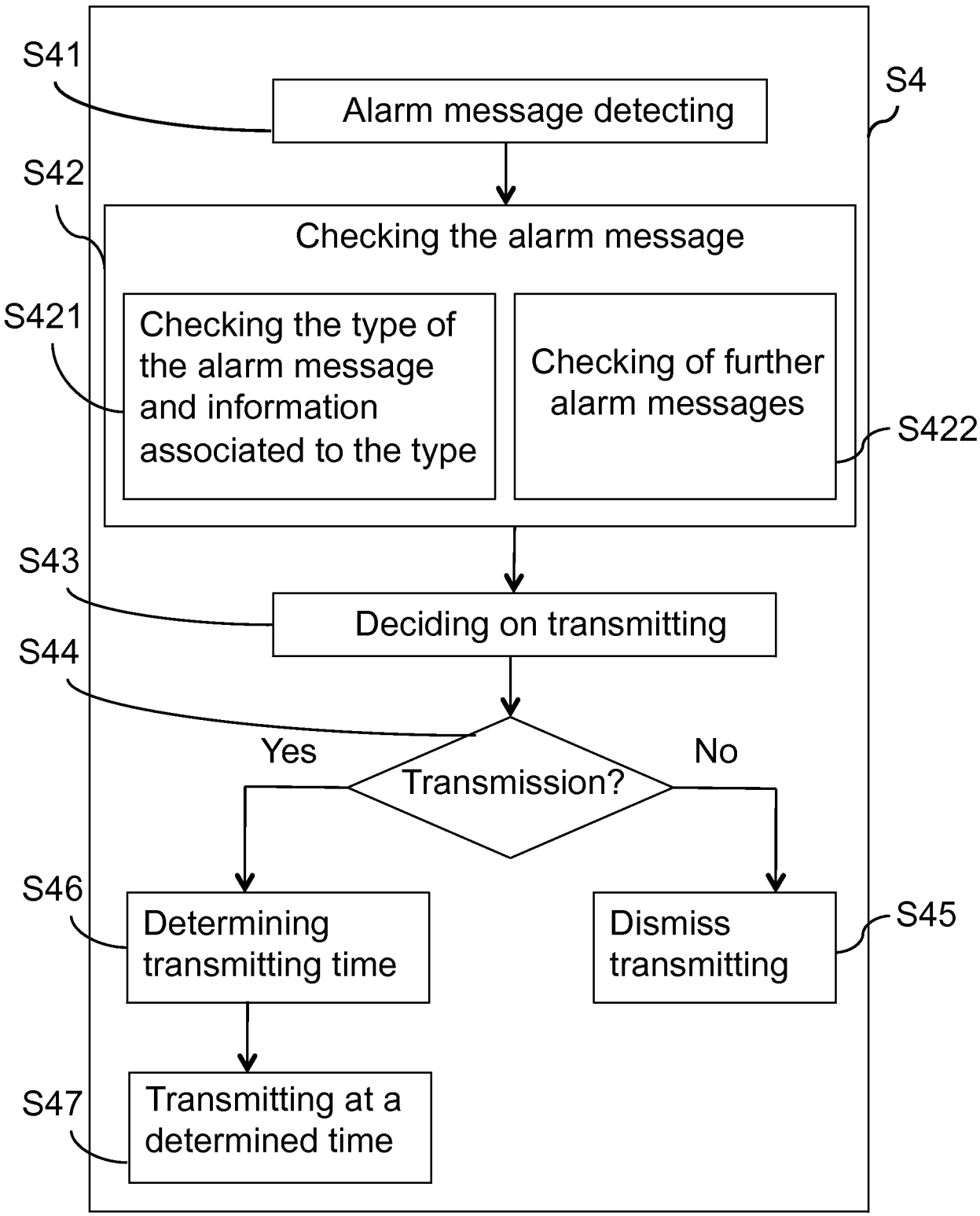
S41
Alarm message detecting
S4
S42
Checking the alarm message
S421
Checking the type of the alarm message and information associated to the type
Checking of further alarm messages
S422
S43
Deciding on transmitting
S44
Yes
Transmission?
No
S46
Determining transmitting time
Dismiss transmitting
S45
S47
Transmitting at a determined time

Fig. 4

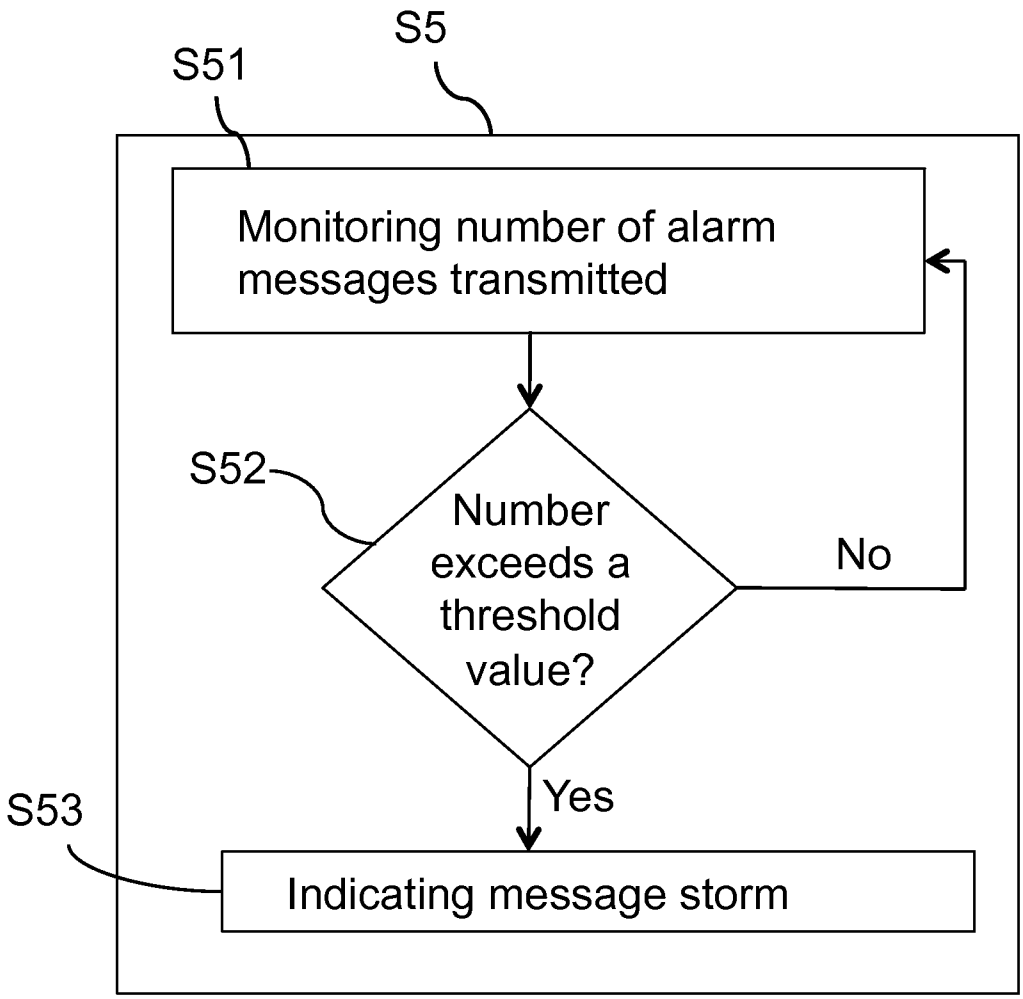
S5
S51
Monitoring number of alarm messages transmitted
S52
Number exceeds a threshold value?
No
Yes
S53
Indicating message storm

Fig. 5

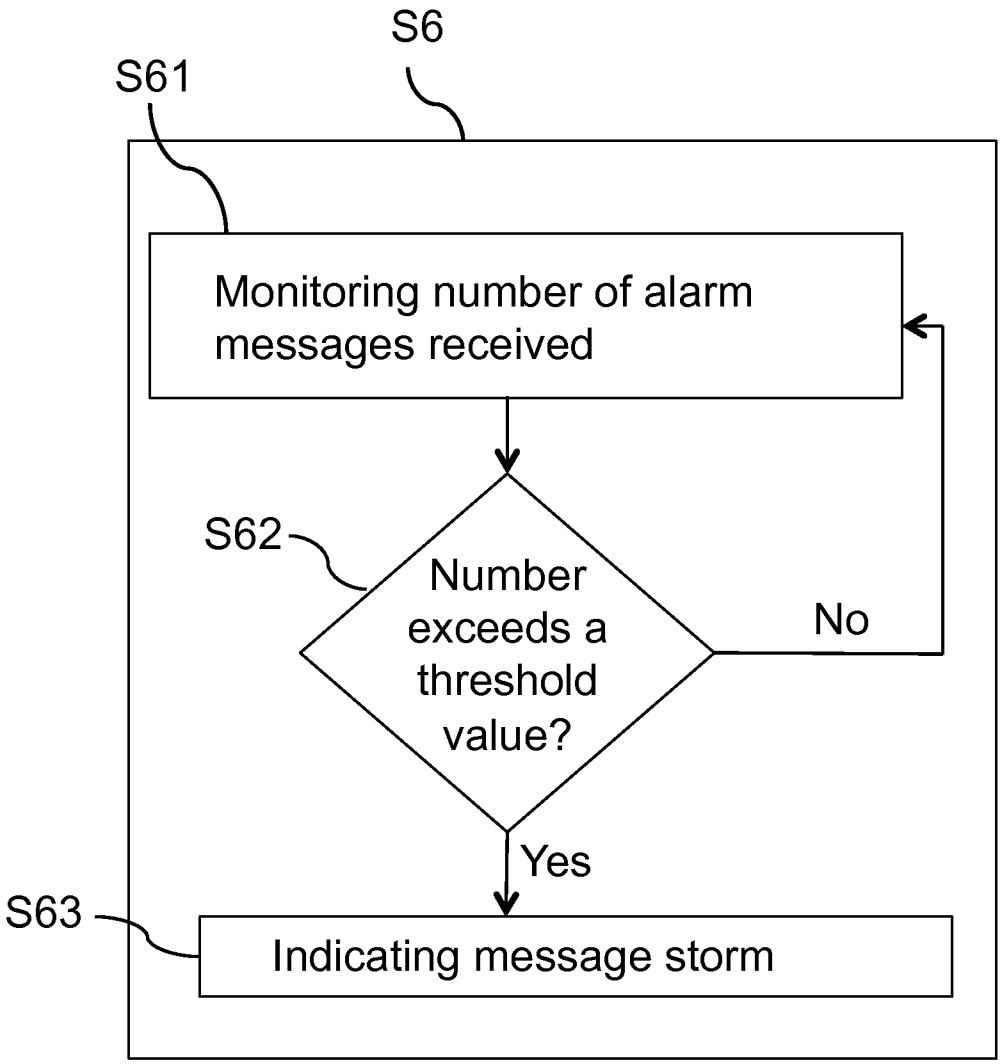
S6
S61
Monitoring number of alarm messages received
S62
Number exceeds a threshold value?
No
Yes
S63
Indicating message storm

Fig. 6

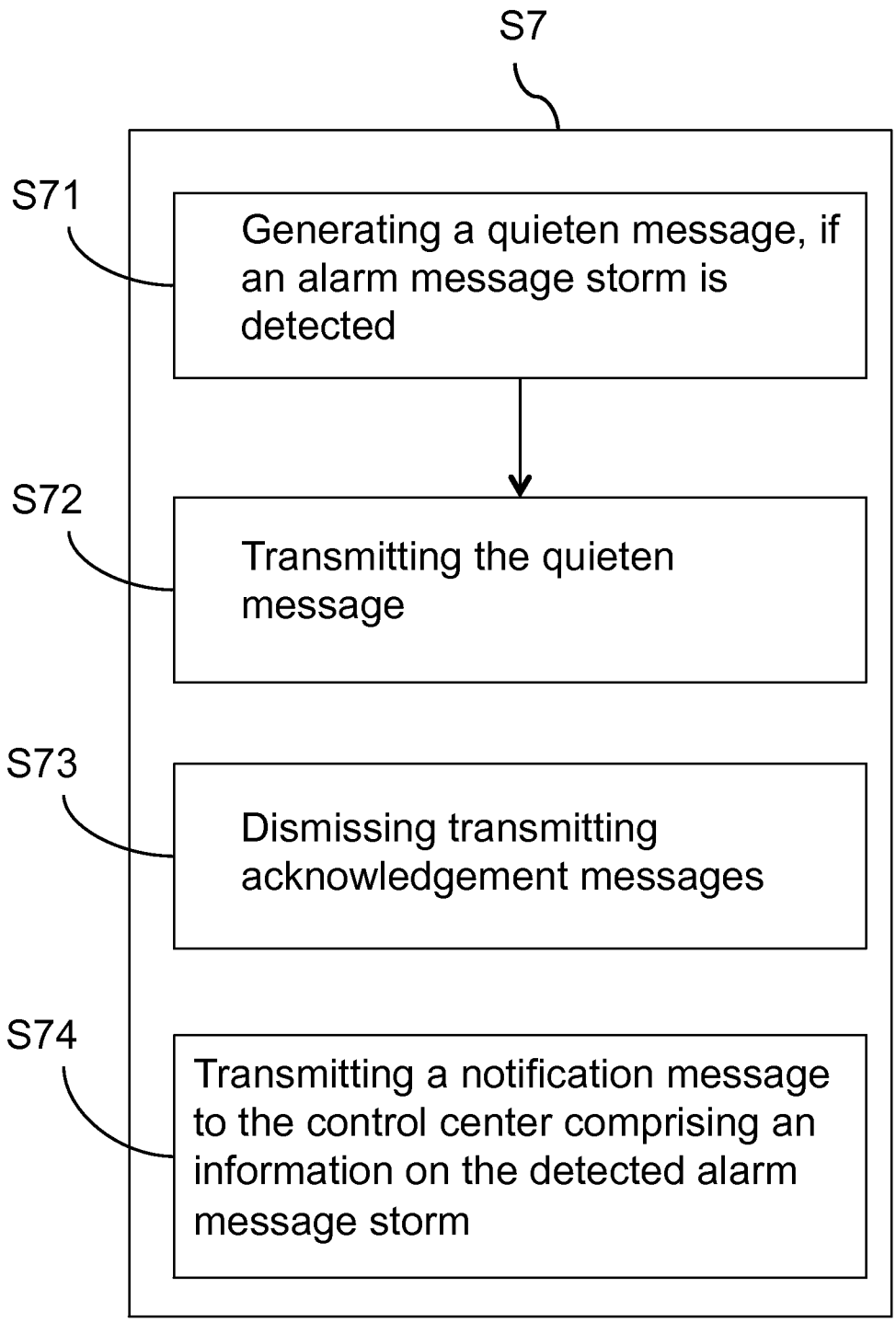
S7
S71
Generating a quieten message, if an alarm message storm is detected
S72
Transmitting the quieten message
S73
Dismissing transmitting acknowledgement messages
S74
Transmitting a notification message to the control center comprising an information on the detected alarm message storm

Fig. 7

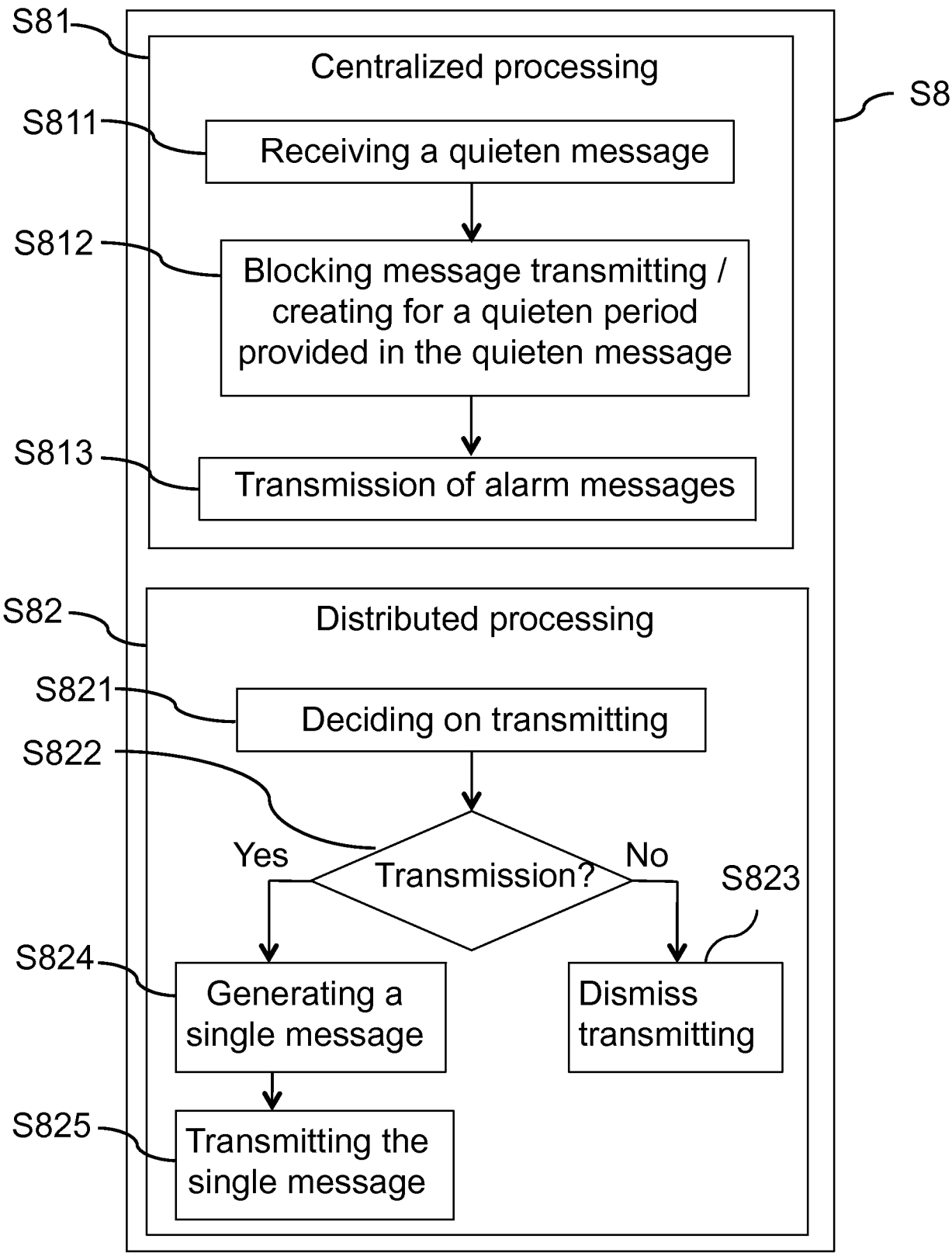
S81
Centralized processing
S8
S811
Receiving a quieten message
S812
Blocking message transmitting / creating for a quieten period provided in the quieten message
S813
Transmission of alarm messages
S82
Distributed processing
S821
Deciding on transmitting
S822
Yes
Transmission?
No
S823
S824
Generating a single message
Dismiss transmitting
S825
Transmitting the single message

Fig. 8

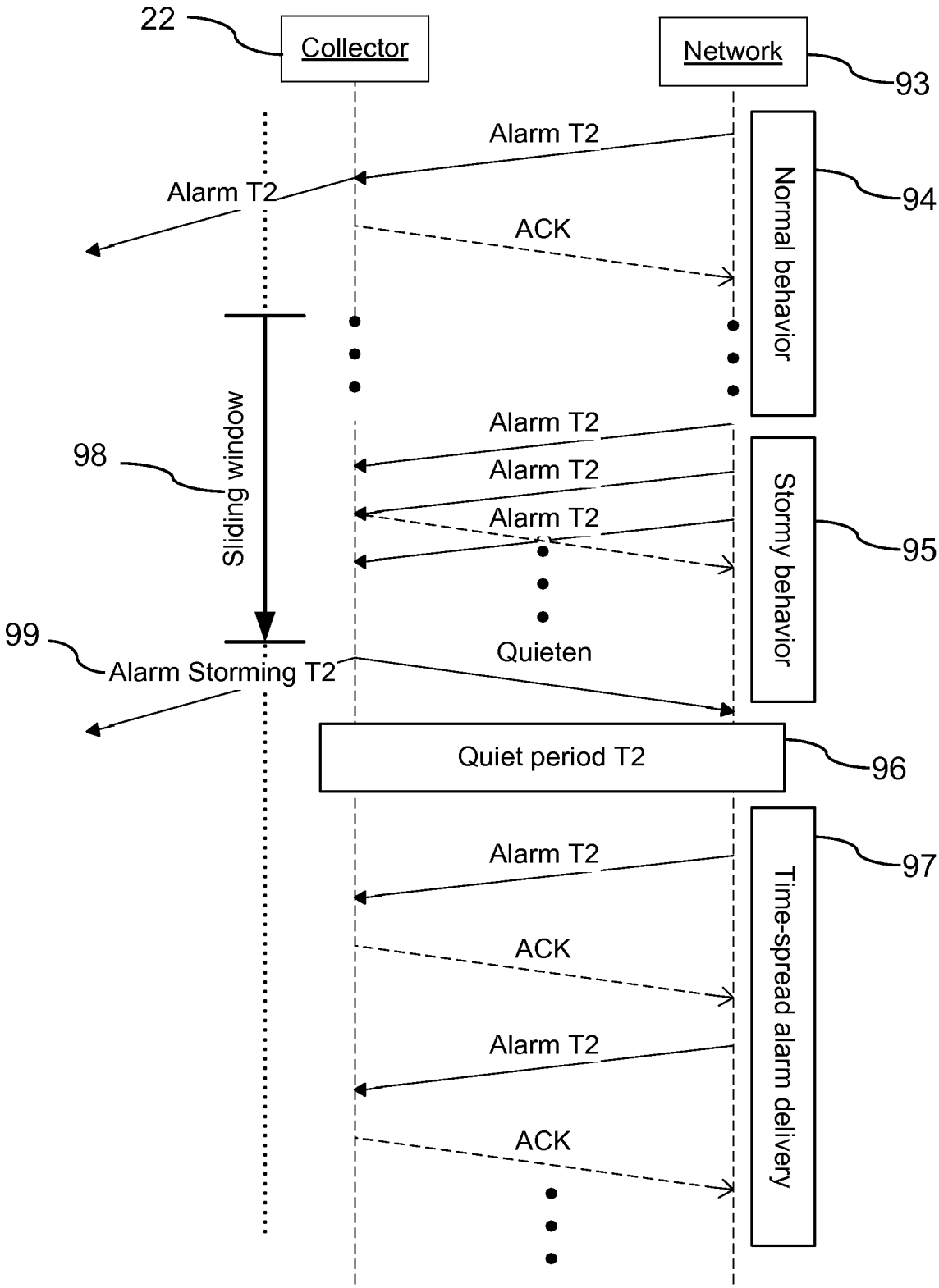
22
Collector
Network
93
Alarm T2
Alarm T2
ACK
Normal behavior
94
Sliding window
98
Alarm T2
Alarm T2
Alarm T2
Stormy behavior
95
99
Alarm Storming T2
Quieten
Quiet period T2
96
Alarm T2
ACK
Alarm T2
ACK
Time-spread alarm delivery
97

Fig. 9

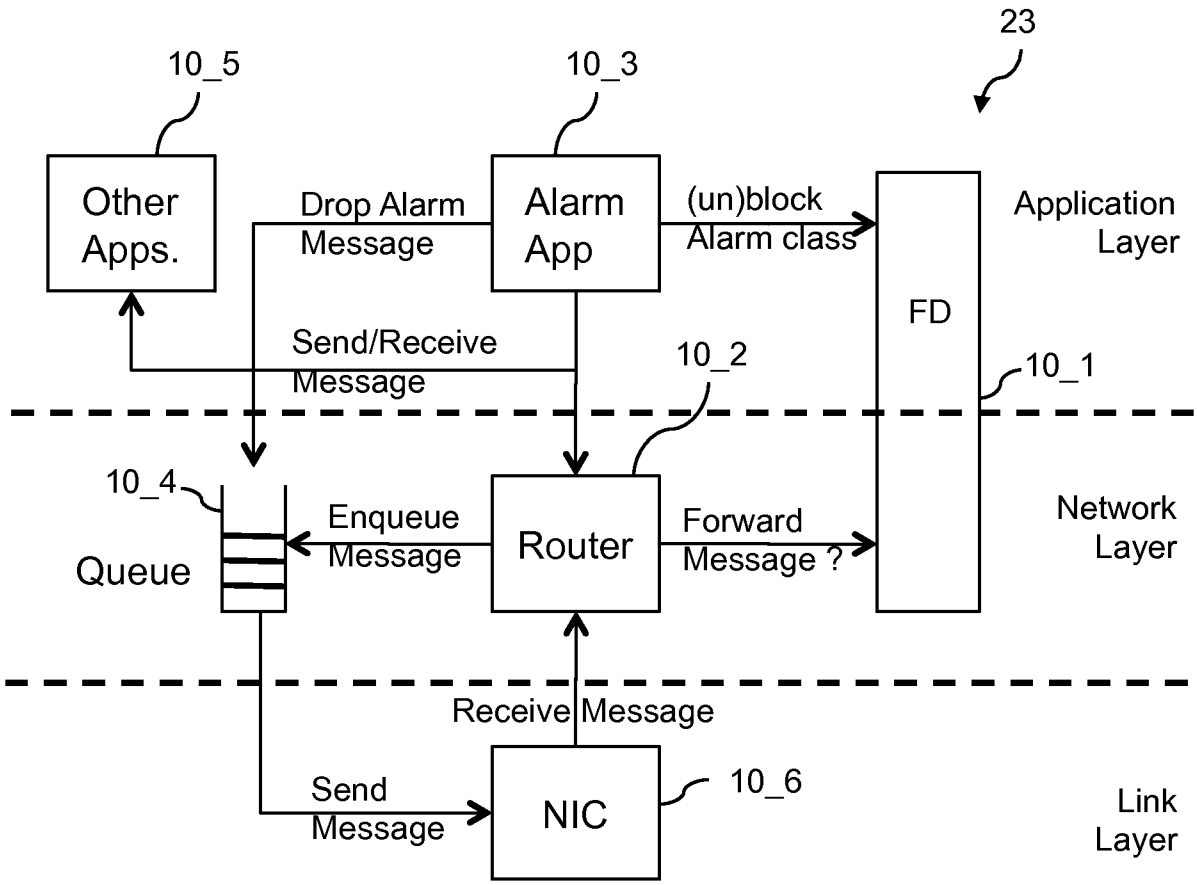
23
10_5
10_3
Other Apps.
Drop Alarm Message
Alarm App
(un)block Alarm class
FD
Application Layer
Send/Receive Message
10_2
10_1
10_4
Queue
Enqueue Message
Router
Forward Message ?
Network Layer
Receive Message
Send Message
NIC
10_6
Link Layer

Fig. 10

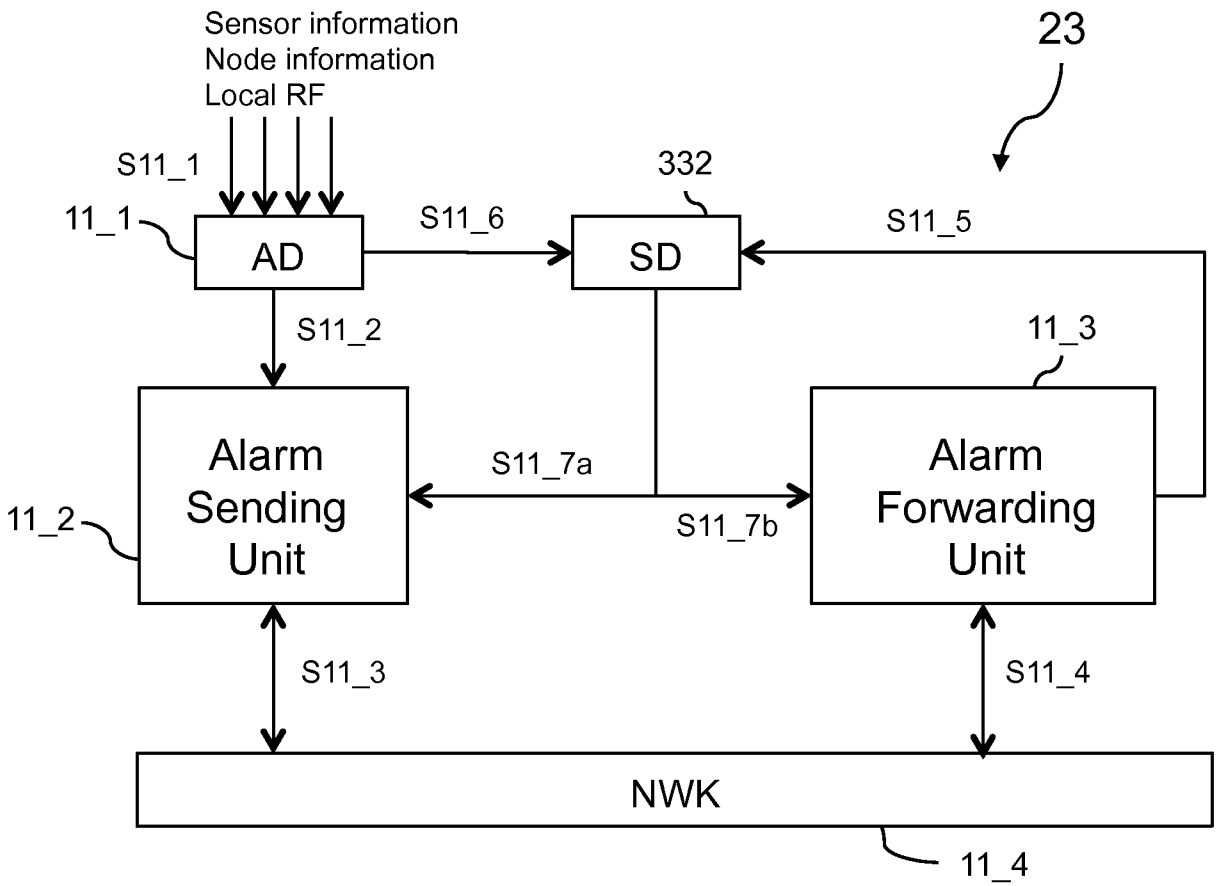
Sensor information
Node information
Local RF
23
S11_1
332
11_1
S11_6
S11_5
AD
SD
S11_2
11_3
Alarm Sending Unit
S11_7a
Alarm Forwarding Unit
11_2
S11_7b
S11_3
S11_4
NWK
11_4

Fig. 11

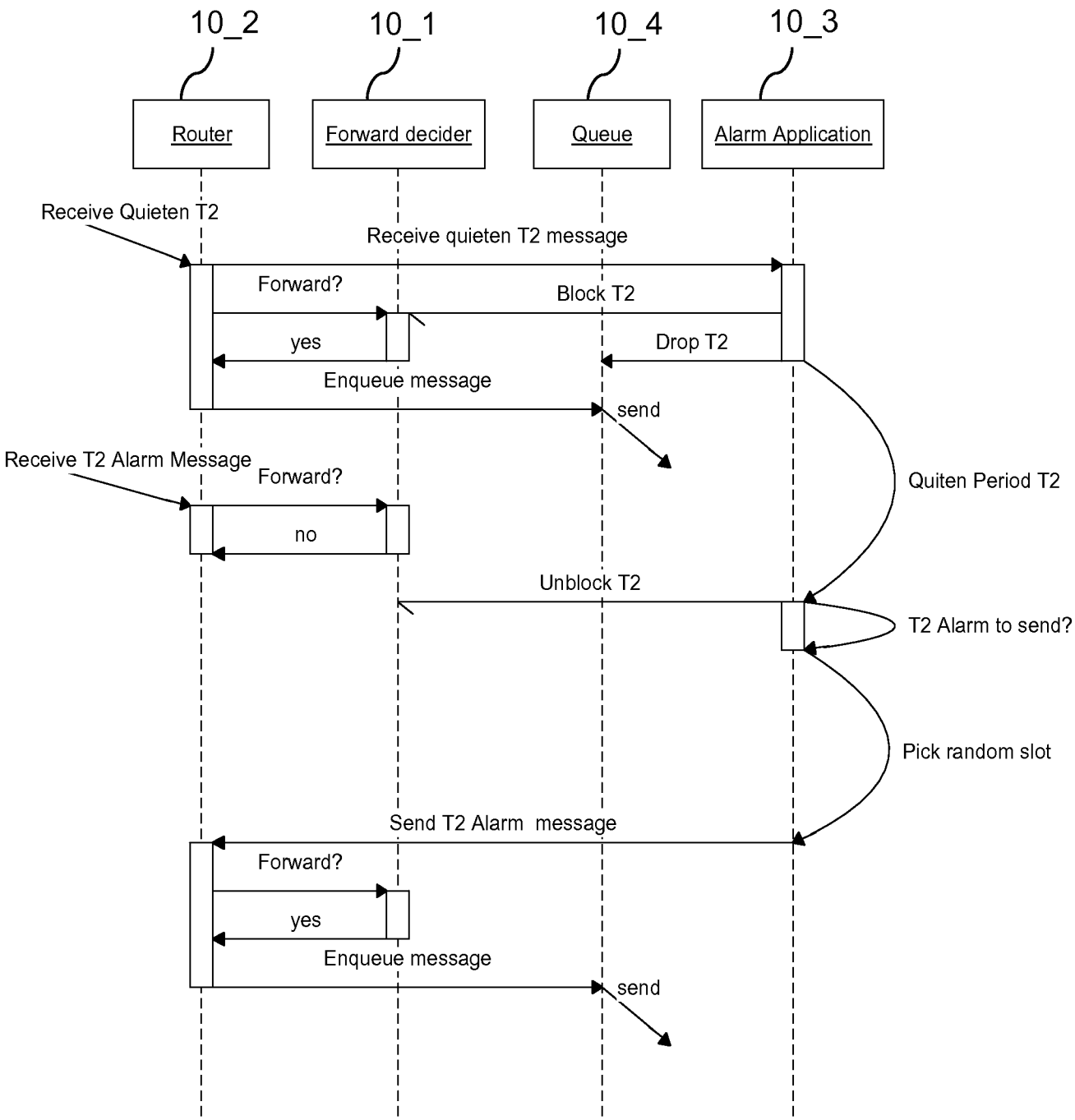
10_2
10_1
10_4
10_3
Router
Forward decider
Queue
Alarm Application
Receive Quieten T2
Receive quieten T2 message
Forward?
Block T2
yes
Drop T2
Enqueue message
send
Receive T2 Alarm Message
Forward?
Quiten Period T2
no
Unblock T2
T2 Alarm to send?
Pick random slot
Send T2 Alarm message
Forward?
yes
Enqueue message
send

Fig. 12