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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2020 (23.07.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/148250 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2020/050752

(22) International Filing Date:
14 January 2020 (14.01.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/CN2019/071648 14 January 2019 (14.01.2019) CN
19158573.6 21 February 2019 (21.02.2019) EP

(71) Applicant: **SIGNIFY HOLDING B.V.** [NL/NL]; High Tech Campus 48, 5656 AE Eindhoven (NL).

(72) Inventors: **DONG, Peiliang**; c/o High Tech Campus 7, 5656 AE Eindhoven (NL). **YAO, Jun**; c/o High Tech Campus 7, 5656 AE Eindhoven (NL). **ZHANG, Zhizhong**; c/o High Tech Campus 7, 5656 AE Eindhoven (NL).

(74) Agent: **SIGNIFY NETHERLANDS B.V.** et al.; VAN EEUWIJK, Alexander, Henricus, Walterus, High Tech Campus 7, 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: METHOD OF AND DEVICE FOR OPERATING A NODE DEVICE IN A COMMUNICATION NETWORK BASED ON CHAINED DATABLOCK TECHNOLOGY

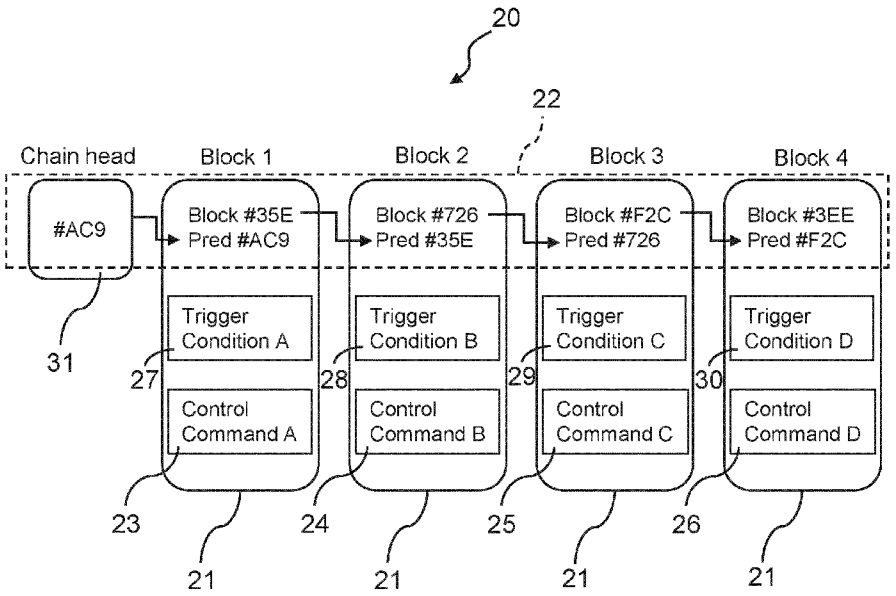


Fig. 2

(57) Abstract: A method, devices and a computer program product for secure operation of node devices of a network of communicatively interconnected node devices, using a chain (20) of datablocks (21). Each datablock (21) of the chain (20) comprises a block hash code (Block #xyz), generated from control data (23-26, 27-30) comprised by a respective datablock and a block hash code (Pred #abc) comprised by a preceding datablock of the chain (20). The block hash codes (Block #xyz) of the chain (20) are available to the node devices. A hash code is generated from control data received at a node device and at least one block hash code available to the node device. If the generated hash code matches a block hash code available to the node device, the node device is operated in accordance with the received control data.

WO 2020/148250 A1

[Continued on next page]

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

Title

Method of and device for operating a node device in a communication network based on chained datablock technology.

Technical Field

The present disclosure generally relates to the operation of a node device in a network and, in particular, to the operation of a node device in a network of communicatively interconnected node devices.

Background

Customer-Premises Equipment, CPE, such as lighting devices having communication capabilities, and Internet of Things, IoT, devices, among which sensors or sensing devices, such as sensors for measuring humidity, temperature, Infra Red, IR, radiation, Carbon Monoxide and/or Carbon Dioxide, generally designated CO_x, actuators, camera systems, alarm systems, are frequently deployed in communication networks comprised of a plurality of communicatively interconnected devices. These devices, generally called node devices, may be movable or mobile devices, operating with a wireless network connection, and/or stationary devices, having either or both a wired and/or wireless network connection. In practice, the term network node device, or in short node device or node, is generic for all such devices.

Networks comprised of communicatively interconnected node devices are also generally called mesh networks, such as Wireless Mesh Networks, WMNs, Wireless Personal Area Networks, WPANs. Network protocols for exchanging data by networked devices or nodes are generally available and known as ZigBee™, Bluetooth™, as well as WiFi based protocols for wireless networks, and wired bus networks such as DALI™ (Digital Addressable Lighting Interface), DSI (Digital Serial Interface), DMX (Digital Multiplex), and KNX (based systems), for example.

In practice, such a network generally comprises multiple network end nodes, network relay nodes, such as bridges, switches and other electric infrastructure devices and equipment, and at least one network control or coordinator device,

generically called a network management device, and/or a gateway device, for providing access to other networks and the Internet, for example.

In a wireless mesh network, a committed node device may communicate with other node devices, network relay nodes or gateway devices in either one of unicast mode and broadcast mode, using the Bluetooth Low Energy, BLE, mesh protocol or the ZigBee protocol, for example, for exchanging, sensing and control information among the node devices, for example. Unless additional authorisation policies or rules are applied in the application layer, a node device may always execute any received valid commands, for example, from any other node devices or a device external to the network.

As a drawback, if an unauthorised user gains control to one of the node devices in a network, the whole network or part thereof may be controlled by that user, by transmitting control commands from that node device to other node devices, for example. In particular in the case of authorised control commands, the node devices will operate in accordance with such control data. If this user also may get access to a network control device, such as a remote controller, in particular in case of a malicious user, that user could harm the intended operation of the network and node devices connected thereto, which may pose severe danger to the whole network. For example, an unauthorised, by an over-the-air, OTA, upgrade or update of node devices, may install malicious software, for taking control or having the device operating with unauthorised control data, for example.

On the other hand, communication modules used in node devices, such as lighting fixtures in a wireless lighting control system, may have very limited hardware resources, i.e. limited memory and/or limited computing power. Other devices may have severe power constraints, such as ultra-low-power switches and some types of sensors which operate with no batteries or which have to guarantee very long battery lives (targeting at 10 years or even longer), thus imposing a very strict regime on their power consumption.

Such power-constrained devices may operate with communication protocols particularly developed, i.e. simplified, for low energy consumption, such as known as EnOcean and ZigBee Green Power, for example. A typical implementation of the above protocols is that the power-constrained device, for example a ZigBee Green Power Device, GPD, sensor sends a broadcast message about its triggering

information, and immediately shuts down its power. Among the neighbour nodes of a GPD, there is at least one router node, called a ZigBee Green Power Proxy, GPP, that translates the received GPD message to a standard ZigBee message, and forwards it to ZigBee Green Power Sink, GPS, devices, either in a unicast or broadcast mode. Typical GPS devices are actuators, which take the required action based on the original information provided by the GPD.

Such a limitation in hardware resources and the use of simplified operating protocols, essentially makes the implementation of complicated security measures in the node devices infeasible.

Accordingly, in practice, there is a need for operating a node device in a network of communicatively interconnected node devices in a more secure and tamper-resist fashion, in particular taking into account the limitations posed by limited hardware resources and/or power-constraint operating protocols.

Summary

The above mentioned and other objects are achieved, in a first aspect of the present disclosure, by a method of controlling a node device of a network of communicatively interconnected node devices, using a chain of datablocks, each datablock of the chain comprising a block hash code, generated in accordance with a hashing scheme from control data comprised by the datablock and a block hash code comprised by a preceding datablock of the chain, wherein the block hash codes of the chain of datablocks are available to the node device, the method being performed by the node device and comprising the steps of:

- receiving control data for controlling the node device;
- generating a hash code from the received control data and at least one block hash code available to the node device, using the hashing scheme;
- verifying the generated hash code with a block hash code available to the node device; and
- operating in accordance with the received control data, if the generated hash code matches a block hash code of the chain of datablocks.

The data chain technology according to the present disclosure enables secure and decentralised network communication and verification of data

exchanged in a peer-to-peer manner. The chain of datablocks essentially comprises a distributed database storing critical information, for which protection is needed as a chain of datablocks. Each datablock contains a part of the information, and the datablocks are chained by back hashes. The chain is distributed over a large number of devices in a network and may be used by these devices to communicate with each other in a secure way.

The topology of a network of communicatively interconnected node devices is advantageously combined with the distributed nature of the data chain technology according to the present disclosure, for controlling a node device comprised in the network. The present disclosure is based on the insight that information critical to the network, such as control data for controlling a node device, may be organised in a distributed manner into a set of datablocks.

Prior to the operation of the network, for example at commissioning thereof, the block content of each datablock is protected from tampering by hashing, for example, based on a cryptographic identifier, a block hash code in this case, of a preceding datablock and the content of the block, i.e. control data or part of the control data applicable in the network, to generate an identifier (a block hash code) to be used by the subsequent datablock to encrypt its block content. By such back hashing, the datablocks are linked into a chain of datablocks. The block hash codes of the datablocks in the chain are made available to the node devices in the network for secure operation of the same.

Upon receiving control data at a node device in the network, the node device verifies the validity of the control data by generating a hash code from the received control data and one of the block hash codes available to or accessible by the node device, and tries to match the thus generated hash code with a block hash code of any one of the datablocks available to the node device.

In the case of a match, i.e. wherein the generated hash code is equivalent to an available block hash code, the received control data may be regarded control data applicable or authorised to use in the network. In the case of a non-match, a new hash code is generated from the received control data and another block hash code available to the node device, different from the previous block hash code, and the new hash code is again compared with the available block hash codes, and so on. The node device only operates in accordance with the received control data when a

match is achieved. In this way, exchanging unauthorised control data among node devices or a worm program or other malicious software or code, not comprised by a datablock of the chain, is effectively prevented, as a hash using such data will not provide a block hash code available to the node devices.

A node device, for operating the method according to the present disclosure, only needs access to the block hash codes of the blocks of the data chain. In practice, these block hash codes occupy limited storage area in local memory of a node device. Further, generating hash codes in accordance with a hashing scheme does not demand powerful processing resources or high power consumption. Accordingly, the method of the present disclosure is very suitable for providing security and tamper-resistivity in node devices having limited hardware resources and/or operating under severe power-constraints.

For the purpose of the present disclosure, commercially available hashing algorithms may be used, such as but not limited to hashing algorithms known under the acronym SHA, Secure Hash Algorithm, such as SHA-256, SHA-512, for example.

The method in accordance with the present disclosure advantageously ensures secure operation of the node device by using the chain of datablocks including the control data, in which integrity of the control data and the datablocks is confirmed by the linking nature of the datablocks provided by the back-hashing of block codes, all the way back to an original genesis datablock.

Due to the back-hash nature of the data structure of the data chain, an alteration of the block content of a datablock in the chain, i.e. the control data, in order to be effective in the network, will need alteration of all subsequent datablocks.

In accordance with an embodiment of the present disclosure, it is advantageous for node devices expected to operate in accordance with the control data authorized in the network, to locally store all block hash codes of the chain of datablocks, which allows the node device to retrieve a block hash code quickly and easily for operating the method according to the present disclosure.

Accordingly, if a node device in a network of node devices in which authorised control data is organised using the above disclosed data chain structure is hacked, an attacker performing the hack may control the hacked node device. However, the other node devices in the network will only operate in accordance with

control data, such as a command, from the hacked node device when that command has been authorised in the data chain, and deny any other commands which may harm the system or cause an unintended operation. Therefore, to control the whole network of node devices operating in accordance with the present disclosure, the attacker has to essentially hack into every node device in the network. This makes breaching of the network very difficult and practically impossible. As a result, secure operation of the node devices is ensured.

Those skilled in the art will appreciate that the block hash codes need not to be stored at each node device operative in the network. Instead, a node device only needs to store the block hash codes containing control data that the node device has to perform.

In accordance with an embodiment of the present disclosure, the block hash codes and the generated hash code are generated from part of the control data, in particular, excluding at least one of command attributes, sequence numbers, error-checking codes, such as Cyclic Redundancy Check, CRC, and encrypted content, for example.

Some information included in the control data of the datablocks may be common to all datablocks, while other information may be specific to only certain datablocks. Such specific information may be excluded from the calculation of the block hash codes and the hash code to be generated.

In accordance with an embodiment of the present disclosure, at least one subset of datablocks of the chain of datablocks is formed required to verify generated hash codes with block hash codes of datablocks comprising data applicable to the node device, the method further comprises performing the steps of generating and verifying based on the at least one subset of datablocks.

Node devices may be configured to only operate with a subset of control data authorized in the network. To reduce the computation load and storage requirements at a particular node device, the hashing and verifying of received control data may be limited to the block hash codes of those datablocks that relate to the control data at which the node device may operate. That is, the datablocks containing the relevant control data and their preceding datablocks. In this case, identifying a subset of datablocks pertaining to the received control data may also help to

significantly reduce the number of attempts required for determining a hash code that matches with one of the block hash codes.

In practice, it is likely that certain control data may comprise a control command which may only be executed under a trigger condition which is also included in the control data. In a further embodiment of the present disclosure, the node device is operating in accordance with the received control data if the generated hash code matches a block hash code of the chain of datablocks and if the trigger condition is met.

Moreover, in the case that the control data comprises a control command together with a trigger condition, the at least one subset of datablocks of the chain of datablocks is identified by at least one of a message ID of a trigger condition, a command ID of a control command, addresses of node devises authorised to send trigger conditions or control commands, and/or hash codes generated from trigger conditions or control commands.

Using properties of the trigger condition and control command, or relating thereto, provides an efficient and easy way of identifying a subset of datablocks of the chain of datablocks which pertains to the received control data. For example when trigger conditions, or a relative simpler hash output of the trigger conditions, are used as an index tool to speed up the hash checking.

The trigger conditions may be physical or non-physical ones. In accordance with an embodiment of the present disclosure, the trigger condition may comprise at least one of a status report from a node device, a key-change report from a node device, a ZigBee Green Power Proxy, GPP, broadcast message containing a status report and a key-change report, and a message with a digital signature from a sender of a control command.

The inclusion of the trigger condition in the control data allows the node device to operate in accordance with the control command in a more flexible way. This is especially beneficial when, in accordance with an embodiment of the present disclosure, at least one of the control data and the block hash codes are stored in at least one of the node devices.

As an example, a sensor or a power constrained node device may generate or evoke a trigger condition and then has the same broadcasted into the network of node devices. Upon receiving the trigger condition, one or more node

devices having full block content of a corresponding datablock including the trigger condition may send a related control command to other node devices which is expected to execute the control command. In this way, scarce resources at node devices need not to be occupied with control data.

In accordance with a further embodiment of the present disclosure, the control data of the chain of datablocks is divided into different subgroups of control data, and the control data of the datablocks of a subgroup is stored in at least one of the node devices.

Such a storage strategy further helps to save the required storage resources for some node devices, which is especially advantageous in case the network comprises large number of node devices with limited storage resources.

In accordance with an embodiment of the present disclosure, the node device may transmit a warning message across the network if the generated hash code does not match with any block hash code available to the node device. In this manner, among others, node devices in the network may become aware of a potential danger present in the network and, if applicable, may switch to a precautionary mode of operation, for example.

A second aspect of the present disclosure provides a node device arranged for operating in a network of communicatively interconnected node devices, using a chain of datablocks, each datablock of the chain comprising a block hash code, generated in accordance with a hashing scheme from control data comprised by the datablock and a block hash code comprised by a preceding datablock of the chain, wherein the block hash codes of the chain of datablocks are available to the node device, the device comprising a receiving module, a generating module, a verifying module and an operating module, wherein:

- the receiving module is arranged for receiving control data for controlling the node device;
- the generating module is arranged for generating a hash code, from the received control data and at least one block hash code available to the node device, using the hashing scheme;
- the verifying module is arranged for verifying the generated hash code with a block hash code available to the node device; and

- the operating module is arranged for operating the node device in accordance with the received control data, if the generated hash code matches a block hash code of the chain of datablocks.

Reference is made to the above elucidating description of the steps of the method according to the first aspect of the present disclosure, for executing of which the node device may be suitably configured. The node device may, in particular, be arranged for operating one of a ZigBee Green Power Device, GPD, a ZigBee Green Power Proxy, GPP, and a ZigBee Green Power Sink, GPS.

A third aspect of the present disclosure provides a device arranged for assigning, in a network of communicatively interconnected node devices, a chain of datablocks, each datablock of the chain comprising a block hash code, generated by hash code generator of the device in accordance with a hashing scheme from control data to be included in the datablock and a block hash code comprised by a preceding datablock of the chain.

In accordance with an embodiment of the present disclosure, the above device is arranged for at least distributing the generated block hash codes to the node devices of the network arranged for operating in accordance with the control data.

Such a device may be provided as a so-called dongle, which is used in connection with a network controller or network management device, to assign during installation and commissioning of the network the chain of datablocks comprising control data authorised for operating a node device of the network and generate the block hash codes. The device thus helps to ensure the security in generating and storing the chain of datablocks in the network.

A fourth aspect of the present disclosure provides a computer program product comprising program code means stored on a computer readable medium, the program code means arranged to perform the above described method, when the program code is executed by at least one computer processor of a node device. The computer program product may be any of a transitory, non-transitory or tangible medium.

A fifth aspect of the present disclosure provides an electric or electronic device, such as a lighting device, comprising at least one node device arranged for operating in accordance with the first aspect of the present disclosure.

These and other aspects of the present disclosure will be apparent from and elucidated with reference to the embodiment(s) described hereinafter.

Brief description of the drawings

Fig. 1 illustrates, schematically, a network of communicatively interconnected network node devices and a gateway device.

Fig. 2 illustrates, schematically, an example of a data chain structure in accordance with the present disclosure.

Fig. 3 illustrates, in a flow chart, an example of detailed steps of a method of operating a node device in accordance with the present disclosure.

Fig. 4 illustrates, schematically, a circuit diagram of an embodiment of a node device in accordance with the present disclosure.

Detailed description

The present disclosure is detailed below with reference to control of ZigBee enabled node devices in a wireless ZigBee™ enabled network. Those skilled in the art will appreciate that the present disclosure is not limited to ZigBee operated networks and devices, but is applicable to a wide variety of networks of communicatively interconnected node devices, either wired and/or wirelessly, and for the exchange of data, such as control command, of application or peripheral devices operatively connected to a node device in the network.

Figure 1 illustrates, schematically, a network 1 of communicatively interconnected network node devices 3, 4, 5, 6, 7, 8 and a gateway device 2.

By way of example, the network 1 shown in Figure 1 is configured as a so-called Wireless Mesh Network, WMN, and is comprised of multiple network end nodes 3, 5, 8 and network relay nodes 4, 6 such as bridges and switches, for example. The nodes 3 - 8 may form part of electric or electronic networked devices. The wireless communication connections between the network devices 2 - 8 are indicated by dashed arrows 9. Those skilled in the art will appreciate that in a general network architecture, node devices may also be connect by wired communication links (not shown).

The network end nodes 3, 5, 8 are generic for supporting data communication of a large variety of electric or electronic devices, either mobile or movable devices and/or non-mobile or stationary devices. Examples of such devices are lighting devices, in particular lighting devices comprising Light Emitting Diode, LED, lighting modules, equipment for mobile telephony and data communication, Customer Premises Equipment, CPE, Internet of Things, IoT, devices, sensor devices, such as sensors for measuring humidity, temperature, Infra Red, IR, radiation, Carbon Monoxide, Carbon Dioxide, generally designated CO_x, actuators, camera systems, alarm systems, etc.

Network relay nodes 4, 6 may bridge a communication distance between neighbouring network end nodes 3, 5 or 5, 8 if such end nodes 3, 5, 8 are not capable of establishing a direct communication connection between these end nodes. It is noted that network relay nodes 4, 6 besides extending the network range, may also support data communication of a same variety of electric or electronic devices as mentioned above in connection with the end nodes 3, 5, 8. Further, an end node and relay node may be comprised in a single physical device. A node device may be mains or battery operated, for example.

The gateway device 2 operates as a network control or coordinator device, which may provide access 11 to other networks, such as the Internet 10, for example. Such a network management, control or coordinator device is also called a backend or network access device. The gateway device 2 may be deployed in the network 1 or remote of the network 1. For communication purposes, the gateway device 2 may comprise integrated transceiver equipment .

For commissioning of the network 1 a so-called communication dongle 12 may be used, that may directly connect to a data processing part of the gateway 2, for example by a universal serial bus, USB, port or the like, and comprises functionality for exchanging data packets or messages with the node devices in the network 1.

The network node devices 3 - 8 may communicate 9 directly with the gateway device 2 or as described above, messages or data packets may be relayed to the gateway device 2 via neighbouring network relay nodes 4 in the mesh network.

The network node devices 3 - 8 are configured for exchanging data messages or data packets with one or a plurality of the node devices in their

neighbourhood, using the same or a different transmission technology. Preferably, the network node devices 3 - 8 and the gateway 2, or the dongle 12, are configured to operate using a same communication technology or protocol. Non-limited examples of applicable transmission protocols are ZigBee™, Bluetooth™, Thread™, EnOcean and ZigBee Green Power, as well as WiFi based protocols and transmission protocols in accordance with a 3GPP standard, and wired bus networks such as DALI™ (Digital Addressable Lighting Interface), DSI (Digital Serial Interface), DMX (Digital Multiplex), and KNX (based systems), wired Ethernet, etc.

Data communication between the node devices 3 - 8 as described above may be controlled by way of a method using the data chain technology in accordance with the present disclosure.

A data chain according to the present disclosure is essentially a distributed database including a chain of datablocks linked by back-hash codes and may be used as a database of records of any kind. Figure 2 illustrates, schematically, an example of a data chain 20 in accordance with the present disclosure. The data chain 20 is a chain of datablocks. For the data chain 20 to be used in the method in accordance with the present disclosure, all authorized control data in the network 1 are to be comprised in the data chain 20. For example, each datablock 21 of the data chain 20 comprises control data including, among others, a control command 23 - 26, for operating a node device 3 - 8 of a network 1 of communicatively interconnected node devices, as illustrated in Figure 1.

In accordance with the data chain structure, each datablock 21 may contain a block header as those illustrated in a dashed rectangle 22 in Figure 2. The block header may comprise a block hash code, indicated by Block #xyz, wherein x, y, z represent hexadecimal characters, and a preceding block hash code, indicated by Pred #abc, corresponding to the block hash code of its preceding datablock, wherein a, b, c represent hexadecimal characters, for example, thereby linking or concatenating the individual datablocks of the chain in a back-hash fashion. The preceding block hash code may also be referred to as a reference hash code. The block control data content may comprise, besides a control command 23 – 26, also a trigger condition 27- 30 for operating a node device, for example.

As an example, a block hash code #AC9 of a chain head 31, also referred to as a genesis block, of the data chain 20 is passed to the next datablock,

block 1, as a Pred block hash code #AC9. Block 1 may generate a block hash code #35E using the Pred block hash code #AC9 from the preceding datablock (the chain head) and its block content, i.e. the control data comprised of the trigger condition A 27 and the control command A 23. The block hash code generated by Block 1 is passed to Block 2 as a Pred block hash code #35E and then used by Block 2 to generate a further block hash code #726, together with its block content including a trigger condition B 28 and a control command B 24 of Block 2. The above procedure is repeated for each datablock to form the chain 20 of datablocks, as illustrated in Figure 2. It is noted that the block hash code of the chain head may be arbitrarily selected, for example.

The block hash codes may be generated in accordance with a hash scheme, i.e. a hash function or hash algorithm. A hash function, in general, is a cryptographic function that takes input of a variable length sequences of a number of bytes x and converts it to a fixed length sequence y. For the data chain, the input of the hash function may be the entire or part of the block content of a datablock, and a hash function such as Secure Hashing Algorithm, SHA-256, or SHA-512 and others may be used to generate the block hash codes of the data chain 20.

For a same network of node devices, a number of different chains of datablocks in accordance with the present disclosure may be used, based on a same or different genesis block and/or as same or different hashing scheme, to contain control data for controlling the node devices of the network and other information.

In accordance with an embodiment of the present disclosure, only part of the block content, i.e. the control data which is common to all trigger conditions or control commands may be included when calculating or computing a block hash code for a datablock, while part of the block content which are specific to each trigger condition or control command is excluded. In an embodiment, specific information may, for example, include sequence numbers, error-checking codes, such as Cyclic Redundancy Check, CRC, or checksum, and encrypted content (which should be decrypted before applying hashing). Moreover, if a class of control commands is to be put in a datablock of the data chain, the differentiating parameters of that class, that is the attributes, may be excluded from hashing. As an example, for a command for setting dimming levels of luminaires, a value of the dimming level may be excluded from hashing.

If a control command can only be sent by a certain node device, an ID of the node device, its address, as an example, may be included in the hashing.

As discussed above, in addition to control commands, datablocks 21 may also contain trigger conditions in their block content for triggering execution of the control commands. In accordance with the present disclosure, the trigger conditions may be physical trigger conditions, such as a status report from a node device like a sensor, a key-change report from a control node, or a ZigBee Green Power Proxy, GPP, broadcast message which contains the above two types of information initiated by a ZigBee Green Power Device, GPD, for example.

In accordance with the present disclosure, if there is no physical trigger condition, for example, when an OTA server initiates an OTA upgrade, the trigger condition in the data chain may be set to a message with a digital signature from a sender of a control command. This can be either a separate message, or a message combining the signature and the command together. In another embodiment of the present disclosure, the trigger condition may be a pre-assigned non-functional message, such as a time stamp, sent by either a sender of a control command or another pre-assigned node, for example. It is also possible that there is no trigger condition.

To be available, block hash codes of all datablocks forming part of the block content may be stored by all node devices, such that they are easily accessible to a respective node device 3 – 8, or may be stored only by those node devices that are expected to execute the control commands. As an example, the block hash codes of all datablocks 21 of the data chain 20 may be stored locally in each node device 3 - 8 in the network 1, or just in a node 3 - 8 that is supposed to execute the authorised control commands.

On the other hand, it is not mandatory for node devices to store the block content of the datablocks, i.e. the trigger conditions, the control commands, the identifying information, and others. To save scarce storage resources at a node device, the block content may be distributed between one or a few node devices of the network, and in a gateway 2 or central control node, for example. In this way, the nodes storing block content can also backup each other.

In still another embodiment, the block content of the data chain may be divided into a few subsets, each subset may have one or several copies of one or

more datablocks respectively, for example, which may then be stored in different nodes 3-8.

Optionally, block content of the datablocks may include identifying information for identifying block content, which may be stored in one or several node devices of the network. In accordance with an embodiment of the present disclosure, the identifying information may be a message ID of a trigger condition; a command ID of a control command; addresses of node devises which are authorised to send trigger conditions or control commands, hash codes generated by block content of trigger conditions or control commands, and combination of any of the above items. It can be appreciated that the identifying information may be formed by other block content of the blocks.

Such a storage strategy helps to speed-up the search time when a node device checking an incoming control command against its stored content of the data chain, which is especially advantageous in a network with many node devices having limited computing power.

It is noted that the distribution of the content of the chain of datablocks, including the block hash codes and block content such as control commands, from and to the network nodes is a sensitive process, which may be protected by other secure measures with a high protecting level, for example, which needs not to be elaborated here.

In the following, the method of controlling a node device according to the present disclosure will be described with reference to Figure 3, which illustrates, in a flow chart, steps of an example of a method 40 of operating a node device in accordance with the present disclosure. For clarity sake, it is assumed that the network 1 is commissioned including the preparation of the data chain and storage of the block chain codes, etc.

The method 40 may start with step 41 where a node device receives a control command for operating the node device, "Receiving a control command for operating node device".

The operation may be configured such that the received control command can only be executed by the node device under a certain trigger condition. In that case, the node device also has to receive that trigger condition, such that the node device may decide whether to execute the control command.

In accordance with the present disclosure, the trigger condition and the control command may be sent separately or together in a same message. In an embodiment where the trigger condition is generated by a sensor or by a power-constrained device, such as a GPD, for example, the trigger condition may be broadcasted into the network firstly. After receiving the trigger condition, one or more nodes that have full block content of a datablock including the trigger condition may transmit a control command corresponding to the trigger condition. In the case of a trigger condition which is a pre-assigned message, it may be handled in the same way as a trigger condition generated by a sensor or a power-constrained device. In another embodiment, the trigger condition may be part of a control command, such as a digital signature or a node ID of a sender of the control command, for example. In this case, both the trigger condition and the control command are automatically sent together.

Next, at step 43, "Generating hash code from a block hash code of one (identified) datablock available to the node device and received control data", the node device receiving the control command for controlling the same determines whether the received control command is authorised or not. To this end, the node device generates a hash code from a block hash code of a datablock in the chain of datablocks available to the node device and the received control command, together with the trigger condition, if available. The hash code is generated using a same hashing algorithm as is used to generate the block hash codes of the data chain 20, as described above.

Following the hashing, at step 44, "Verifying generated hash code with block hash code available to node device", the generated hash code is compared to block hash codes of the data chain 20 to identify a block hash code that matches the generated hash code. If there is no match, a new hash code is generated, by the node device, from another, i.e. a different, block hash code of a datablock in the chain of datablocks available to the node device and the received control command and trigger condition if applicable, and this new hash code is again compared with the available block hash codes. If there is a match, the validity of the control command is acknowledged and the control command may be executed by the node device subsequently, if applicable dependent on a trigger condition.

Optionally, in accordance with the present disclosure, identifying information of the block content which is stored by some node devices may be used

to speed-up the matching process. In an embodiment, to find a matched datablock, the node device may, at step 42, "Identifying datablocks pertaining to received control data", search the identifying information of each datablock firstly. Then the node device only hashes the block content of the datablocks which have matched the identifying information. In this manner, the total number of hashing attempts can be significantly reduced.

In the case that a matching is achieved, i.e. step 45 "Match ?", result "Yes", the node device at step 46, "Operating node device in accordance with control data", is enabled for operating in accordance with the control command, to dim the light, for example.

Optionally, in an embodiment of the present disclosure, if the received trigger condition and control command cannot match with any datablock in the data chain, i.e. step 45 "Match ?", result "No", the node device receiving the control command may, at step 47, "Transmitting warning message", send a broadcast across the whole network about the mismatch, which may arise from a potential tampering, for example, so that other node devices can stop executing the command. That is, a veto message may be send in the network by the node devices receiving the invalid control command. A digital signature may be added in this veto message, to avoid fake vetoes.

Due to the back-hash nature of the data structure of the data chain, an alteration to the block content of one datablock in the data chain, such as an alteration of a control command, for example, to be executed by a control node, will need alteration of all subsequent datablocks.

If a node device in a network of node devices in which authorised control data is organised using the above disclosed data chain structure is hacked, an attacker performing the hack may control the hacked node device. The other node devices will only operate in accordance with a control command from the hacked node device when that control command has been authorised in the data chain. Non-authorised control commands will result in the generation of hash codes unknown in the network, hence will be ignored and may not harm the system. Therefore, to control the whole network of node devices protected in accordance with the present disclosure, the attacker has to ultimately hack every node device in the network. This

makes malicious network operation due to the tampering very difficult and practically impossible.

The above method 40, in accordance with an embodiment of the present disclosure, therefore allows the network of node devices to be tamper resistant by employing verification of a received control command and other information for controlling the node devices using the data chain scheme disclosed. Distribution of the block hash codes of the data chain to all the node devices, and the storage of other information at only a limited number of node devices with sufficient storage resources, for example, is beneficial in that the node devices with limited resources may still be securely protected from an attack.

In the unlikely event that tampering does happen, for example when an attacker has hacked a network device and got the network key, functions available to the attacker are only limited to what has been authorised to a network device by the data chain 20.

The attacker might try to modify the block content in the data chain. However, due to the properties of hash computation, it is almost impossible to modify the block content of a datablock without changing the block hash codes of the data chain. Moreover, if the block hash code of a datablock has been changed, the block hash codes of all the following blocks have to be changed as well. To achieve these changes, the attacker has to either distribute a new data chain to overwrite the old one, or has to hack into every network node of the network.

Note that the command to initiate a re-distribution is very likely to be protected, i.e. included in the data chain as well, and the hacked node even may not have the authority to initiate a re-distribution. Hacking the network devices one by one, will take a very long time and effort, which gives the system owner a good chance to discover the attack.

Figure 4 illustrates, schematically, a circuit diagram of an embodiment of a node device in accordance with the present disclosure. The node device 50 comprises a transceiver, Tx/Rx, module 51 arranged for a wireless 52 or wired 53 exchange of messages or data packets with a gateway and/or other node devices, inclusive relay node devices, in a network of communicatively interconnected network node devices. The transceiver 51 may be configured to operate in accordance with

any of the data communication technologies and protocols mentioned above with reference to Figure 1, in one or both of a broadcast and unicast mode of operation.

The node device 50 further comprises at least one data processor or controller 55, and at least one data repository or storage or memory 56, among others for storing computer program code instructions which, when loaded and run on to the one or more processor or controller 55, configure the node device 50 to operate in accordance with the present disclosure. Address information 57 of the node device in a network, inclusive its MAC address, may be stored in the repository 56, or a separate memory or storage accessible to the at least one processor or controller 55. The at least one processor or controller 55 communicatively interacts with and controls the transceiver 51 and the at least one repository or storage 56 via an internal data communication bus 58 of the node device 50.

The node device 50 may be part of or operatively connect 54 to an electric or electronic device, such as lighting device 60, comprising a lighting module 61, preferably a LED lighting module, operation of which may be controlled by the node device 50 from or through a network gateway, or by a remote control device, for example. As mentioned above, instead of or in addition to a lighting device, a node device may control several other electric or electronic devices, operatively connected in a network in accordance with the present disclosure.

The node device 50 may be arranged for operating, in a securely and tamper-resistant fashion, in a network of communicatively interconnected node devices, such as illustrated in Figure 1, using a chain of datablocks described above with reference to Figure 2. For this purpose, the node device 50 may further comprise a receiving module 62, a generating module 63, a verifying module 64 and an operating module 65, all operatively connected to the internal data communication bus 58.

In accordance with the present disclosure, the receiving module 62 may be arranged for receiving control data for operating the node device 50. The generating module 63 may be arranged for consecutively generating a hash code, from the received control data and a block hash code available to the node device, using a hashing scheme as described above. The verifying module 64 may be arranged for matching the generated hash code with a block hash code available to the node device 50. The operating module 65 may be arranged for operating the node device 50 in

accordance with the received control data, if the generated hash code matches a block hash code of the chain of datablocks.

Block hash codes may be available to the node device 50 from the network, such as another node device in the network, through the transceiver 51, or directly stored 66 in the data repository or storage or memory 56.

The receiving module 62 may further be arranged for receiving a trigger condition for triggering transmission of the control command to the node device 50. The trigger condition may be sent to the node device 50 together with or prior to the control command.

In accordance with an embodiment of the present disclosure, the transceiver module 51 of the node device 50 may be arranged for transmitting a warning message across the network if none of the generated hash codes matches with any block hash code available to the node device 50.

It is likely that a node device of a network may have a communication module, such as the transceiver module 51, with limited hardware resources. As an example, a power-constrained device such as ZigBee Green Power Device, GPD may send a broadcast message about its triggering information, and immediately shuts down its power. Among neighbouring nodes of a GPD, there may be at least one router node which is called ZigBee Green Power Proxy, GPP. A GPP node may translate the GPD message to a standard ZigBee message, and forward it to ZigBee Green Power Sink, GPS, devices, either by unicasts or broadcasts. The GPS devices are actuators which take the further actions based on the original information provided by the GPD.

The node device 50 in accordance with the present disclosure may be advantageously used to operate the above ZigBee GPD, ZigBee GPP, and ZigBee GPS by allowing the devices with limited storage resource and low power consumption to store only the block hash codes, while storing the other block content to other node devices having better storage capacity.

In accordance with the present disclosure, during installation and commissioning of a network, such as the network 1 shown in Figure 1, a so-called dongle 12 may function as a chain manager of a data chain to be used by the network 1 for security purposes. In an embodiment of the present disclosure, the dongle 12 may be arranged for generating the block hash codes of the data chain. The dongle 12 may also assign the data chain-protected control commands. The data chain may

include a command of re-distributing the data chain to the network, in case a new node device is added to the network, as an example. In the case that the dongle 12 is used to generate the block hash codes, a trigger condition should include that a sender of a control command must be the chain manager, i.e. the dongle 12.

The chain manager may then distribute the data chain in the network, with the block hash codes being delivered to every node device in the network, while the full block content, including trigger conditions, control commands and possibly identifying information, is divided into a few subsets, and separately stored in a number of different nodes. Each subset may have one or several copies in one or several nodes, respectively.

After installation, an owner of the network may switch off the chain manager, and place it in a safe place which is inaccessible to unauthorised people. Only if the data chain needs to be modified and re-distributed, the owner turns on the chain manager and perform the required works.

In such a network, an attacker has to either get access to the chain manager, or hack into every one of the network nodes, to get the full control of the network. Secure operation of node devices of the network is thereby ensured.

It is noted that the above devices may be implemented based on discrete hardware circuitries with discrete hardware components, integrated chips, or arrangements of chip modules, or based on signal processing devices or chips controlled by software routines or programs stored in memories, written on a computer readable media, or downloaded from a network, such as the Internet.

For example, the operation of the receiving module 62, generating module 63,verifying module 64 and operating module 65, of the node device 50 may be completely or partly performed by the processor or controller 55 of a node device 50.

It shall be understood that the devices, the commissioning and/or control device, a luminaire device, a lighting system, the method, and the computer program product of the above aspects may have similar and/or identical preferred embodiments, in particular, as defined in the dependent claims.

It shall be understood that a preferred embodiment of the present disclosure can also be any combination of the dependent claims or above embodiments with the respective independent claim.

Claims

1. A method (40) of controlling a node device (3-8) of a network (1) comprising a plurality of node devices, using a chain (20) of datablocks (21), each datablock of said chain (20) comprising a block hash code (Block #xyz), generated in accordance with a hashing scheme from control data comprised by said datablock and a block hash code (Pred #abc) comprised by a preceding datablock of said chain (20), wherein said block hash codes of said chain of datablocks are available to said node device, said method performed by said node device and comprising the steps of:

- receiving (41) control data for controlling said node device;
- generating (43) a hash code from said received control data and at least one block hash code available to said node device, using said hashing scheme;
- verifying (44) said generated hash code with a block hash code available to said node device; and
- operating (46) in accordance with said received control data, if said generated hash code matches (45) a block hash code of said chain of datablocks.

2. The method according to claim 1, wherein said block hash codes and said generated hash code are generated from part of said control data, in particular, excluding at least one of command attributes, sequence numbers, error-checking codes, CRC, and encrypted content.

3. The method according to claim 1 or 2, wherein at least one subset of datablocks of said chain of datablocks is formed (41) required to verify generated hash codes with block hash codes of datablocks comprising control data applicable to said node device, said method further comprising performing said steps of generating (43) and verifying (44) based on said at least one subset of datablocks.

4. The method according to any of the previous claims, wherein said control data comprises a trigger condition (27-29) and a control command (23-26), and said node device is operating in accordance with said received control data if said generated hash code matches a block hash code of said chain of datablocks (20) and said trigger condition is met.

5. The method according to claim 4 dependent on claim 3, wherein at least one subset of datablocks of said chain of datablocks is identified by at least one of a message ID of a trigger condition (27-29), a command ID of a control command (23-26), addresses of node devises authorised to send trigger conditions or control commands, hash codes generated from trigger conditions or control commands.

6. The method according to claim 5, wherein said trigger condition (27-29) comprises at least one of a status report from a node device, a key-change report from a node device, a ZigBee Green Power Proxy, GPP, broadcast message containing said status report and said key-change report, and a message with a digital signature from a sender of a control command.

7. The method according to any of the previous claims, wherein at least one of said control data and said block hash codes are stored in at least one of said node devices (3-8).

8. The method according to any of the previous claims, wherein said control data of said chain (20) of datablocks is divided into different subgroups of control data, and wherein said control data of said datablocks of a subgroup is stored in at least one of said node devices (3-8).

9. The method according to any of the previous claims, further comprising transmitting a warning message (47) across said network if said generated hash code does not match with any block hash code available to said node device.

10. A node device (50) arranged for operating in a network (1) of communicatively interconnected node devices, using a chain (20) of datablocks (21), each datablock of said chain (20) comprising a block hash code (Block #xyz), generated in accordance with a hashing scheme from control data comprised by said datablock and a block hash code (Pred #abc) comprised by a preceding datablock of said chain (20), wherein said block hash codes of said chain of datablocks are available to said node device (50), said node device comprising a receiving module

(62), a generating module (63), a verifying module (64) and an operating module (65), wherein:

- said receiving module (62) is arranged for receiving control data for controlling said node device;
- said generating module (63) is arranged for generating a hash code from said received control data and at least one block hash code available to said node device, using said hashing scheme;
- said verifying module (64) is arranged for verifying said generated hash code with a block hash code available to said node device; and
- said operating module (65) is arranged for operating said node device in accordance with said received control data, if said generated hash code matches a block hash code of said chain of datablocks.

11. The node device according to claim 10, further arranged for operating in accordance with any claims 2 to 9, in particular, wherein said node devices of said network are arranged for operating one of a ZigBee Green Power Device, GPD, a ZigBee Green Power Proxy, GPP, and a ZigBee Green Power Sink, GPS.

12. A device (12) arranged for assigning, in a network (1) comprising a plurality of node devices (3-8), a chain (20) of datablocks (21), each datablock of said chain (20) comprising a block hash code (Block #xyz), generated by hash code generator of said device in accordance with a hashing scheme from control data to be included in said datablock and a block hash code (Pred #abc) comprised by a preceding datablock of said chain (20).

13. The device according to claim 12, arranged for at least distributing said generated block hash codes to said node devices of said network arranged for operating in accordance with said control data.

14. A computer program product comprising program code means stored on a computer readable medium, said program code means arranged to perform said method according to any of claims 1 to 9, when said program code is executed by at least one computer processor of a node device.

15. An electric or electronic device (60), such as a lighting device, comprising at least one node device (50) according to any of claims 10 or 11.

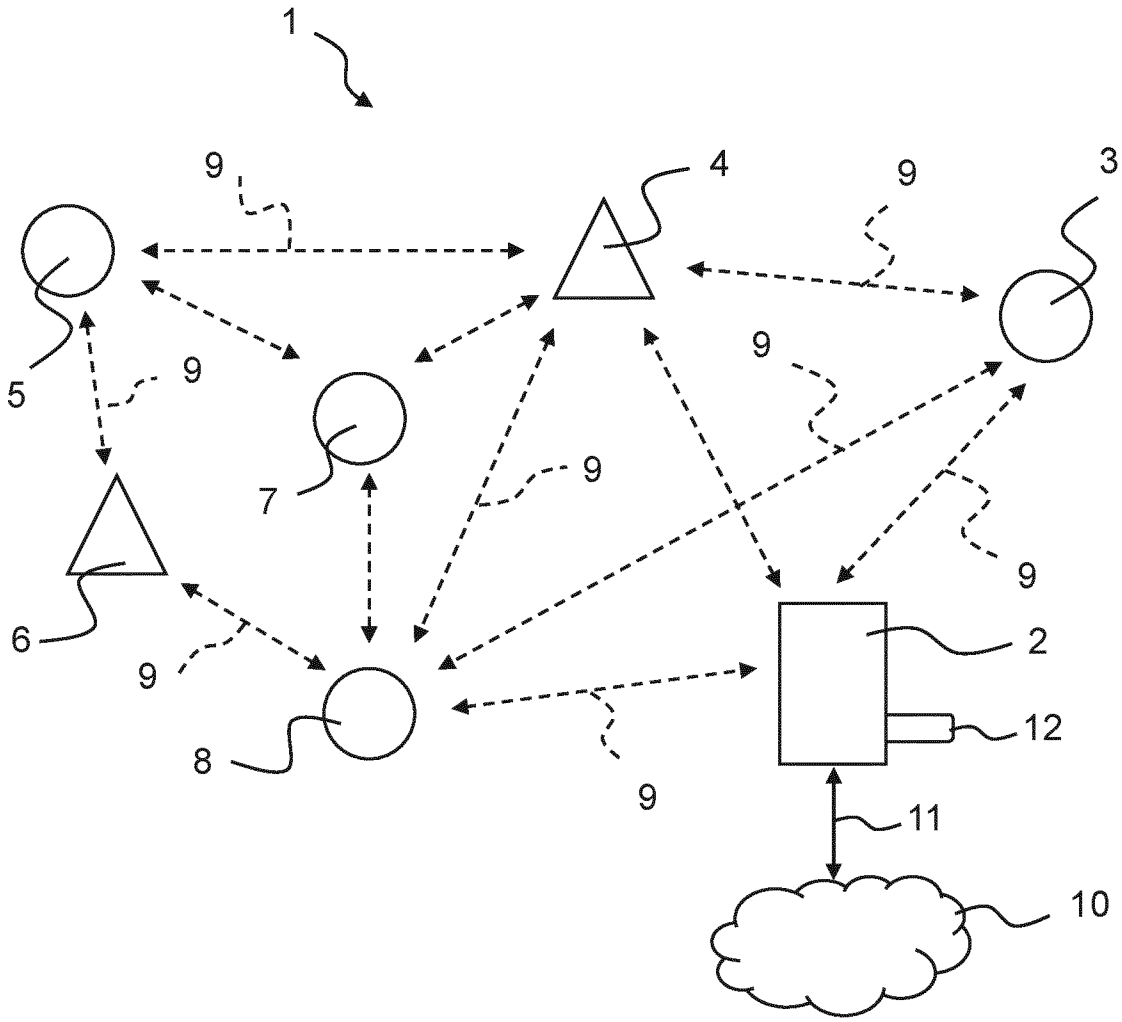


Fig. 1

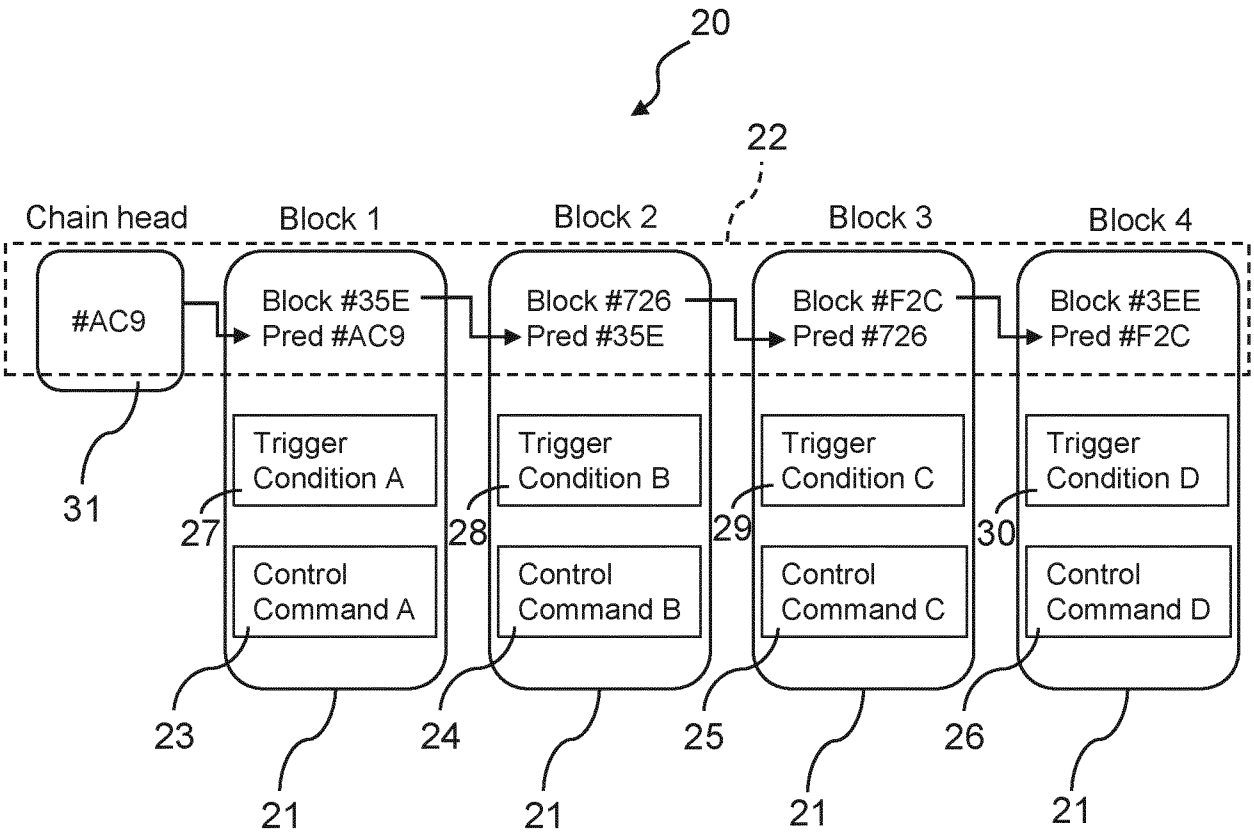

20
22
Chain head
Block 1
Block 2
Block 3
Block 4
#AC9
Block #35E
Pred #AC9
Block #726
Pred #35E
Block #F2C
Pred #726
Block #3EE
Pred #F2C
Trigger
Condition A
Trigger
Condition B
Trigger
Condition C
Trigger
Condition D
Control
Command A
Control
Command B
Control
Command C
Control
Command D
31
27
28
29
30
23
24
25
26
21
21
21
21

Fig. 2

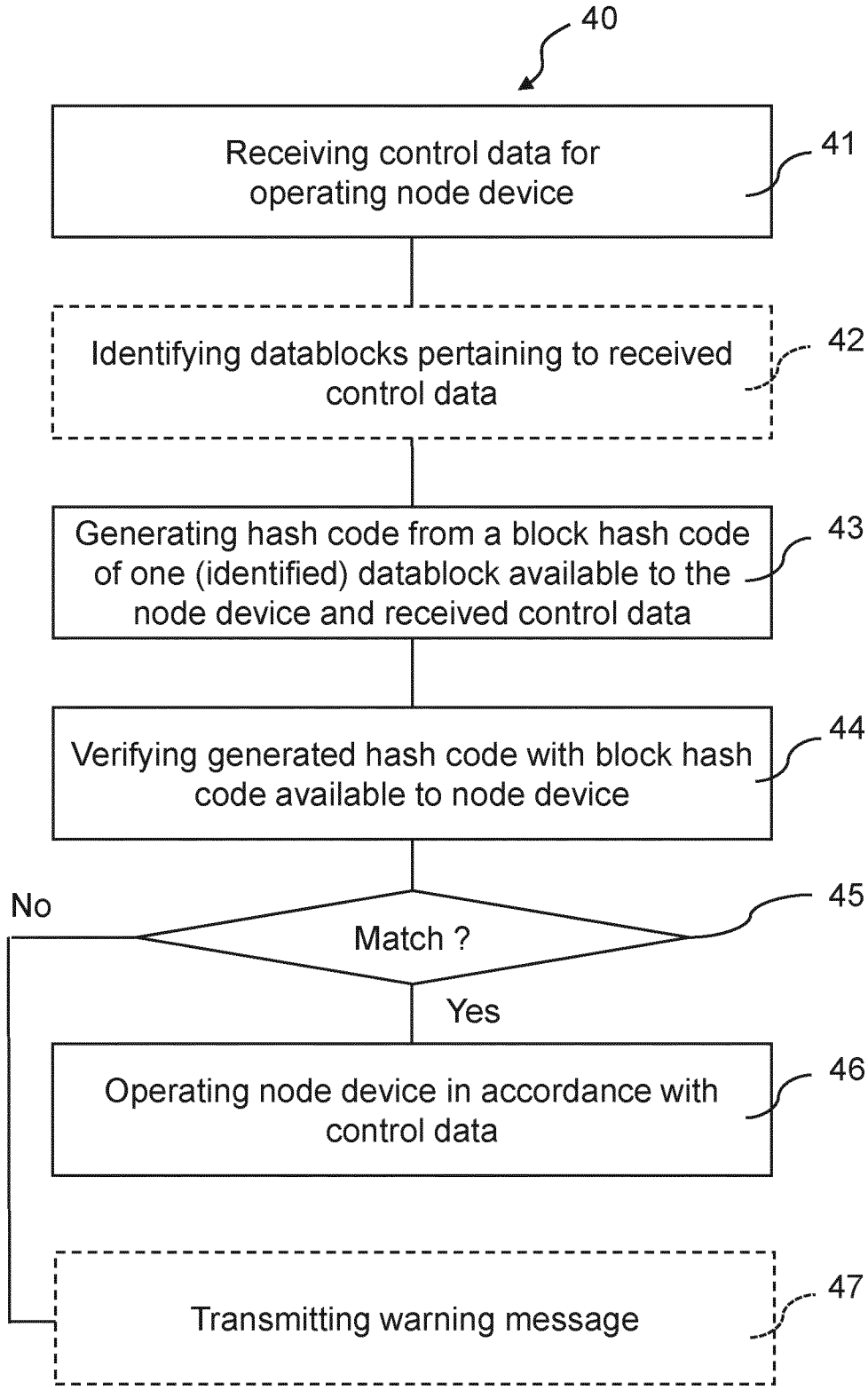

40
Receiving control data for operating node device
41
Identifying datablocks pertaining to received control data
42
Generating hash code from a block hash code of one (identified) datablock available to the node device and received control data
43
Verifying generated hash code with block hash code available to node device
44
Match ?
45
No
Yes
Operating node device in accordance with control data
46
Transmitting warning message
47

Fig. 3

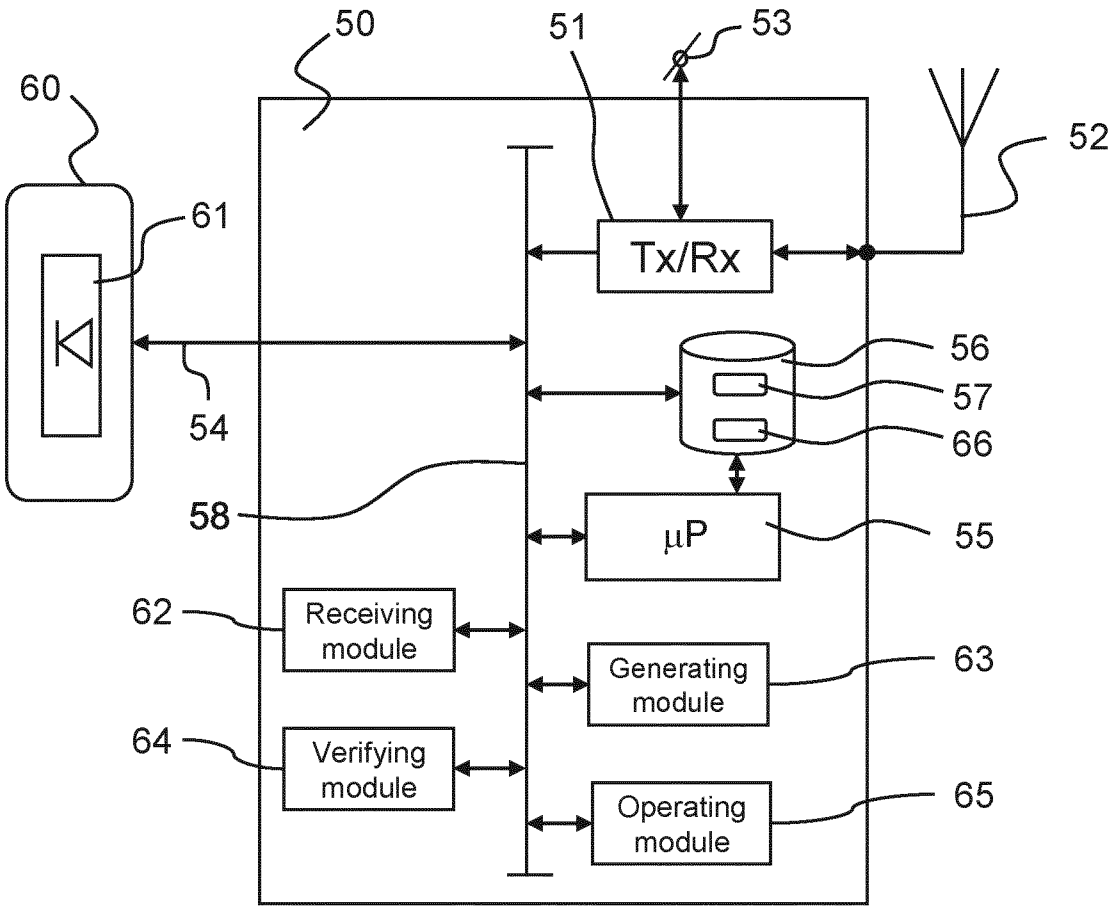

50
51
53
60
52
61
Tx/Rx
56
57
54
66
58
µP
55
62
Receiving module
63
Generating module
64
Verifying module
65
Operating module

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/050752

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06F

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

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

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2018/254905 A1 (CHUN SAM GU [KR]) 6 September 2018 (2018-09-06) abstract paragraphs [0002] - [0081] figures 1-4	1-15

X	ZHANG XIAOHONG ET AL: "Blockchain-Based Secure Equipment Diagnosis Mechanism of Smart Grid", IEEE ACCESS, vol. 6, 24 July 2018 (2018-07-24), pages 66165-66177, XP011696870, DOI: 10.1109/ACCESS.2018.2856807 the whole document	1-15

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 February 2020	13/02/2020

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

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/050752

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 3 396 575 A1 (ACCENTURE GLOBAL SOLUTIONS LTD [IE]) 31 October 2018 (2018-10-31) abstract paragraphs [0002] - [0132] figures 1-16 -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/050752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018254905 A1	06-09-2018	EP 3386142 A1	10-10-2018
		JP 6601828 B2	06-11-2019
		JP 2018525952 A	06-09-2018
		KR 101678795 B1	22-11-2016
		US 2018254905 A1	06-09-2018
		WO 2017095036 A1	08-06-2017
EP 3396575 A1	31-10-2018	AU 2018202523 A1	15-11-2018
		CN 108805703 A	13-11-2018
		EP 3396575 A1	31-10-2018
		US 2018314809 A1	01-11-2018
		US 2019108323 A1	11-04-2019
		US 2019266312 A1	29-08-2019