Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2748483 C 2016/05/03

(11)(21) **2 748 483**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2010/01/12
(87) **Date publication PCT/PCT Publication Date:** 2010/07/22
(45) **Date de délivrance/Issue Date:** 2016/05/03
(85) **Entrée phase nationale/National Entry:** 2011/06/28
(86) **N° demande PCT/PCT Application No.:** EP 2010/050273
(87) **N° publication PCT/PCT Publication No.:** 2010/081798
(30) **Priorité/Priority:** 2009/01/15 (EP09150630.3)

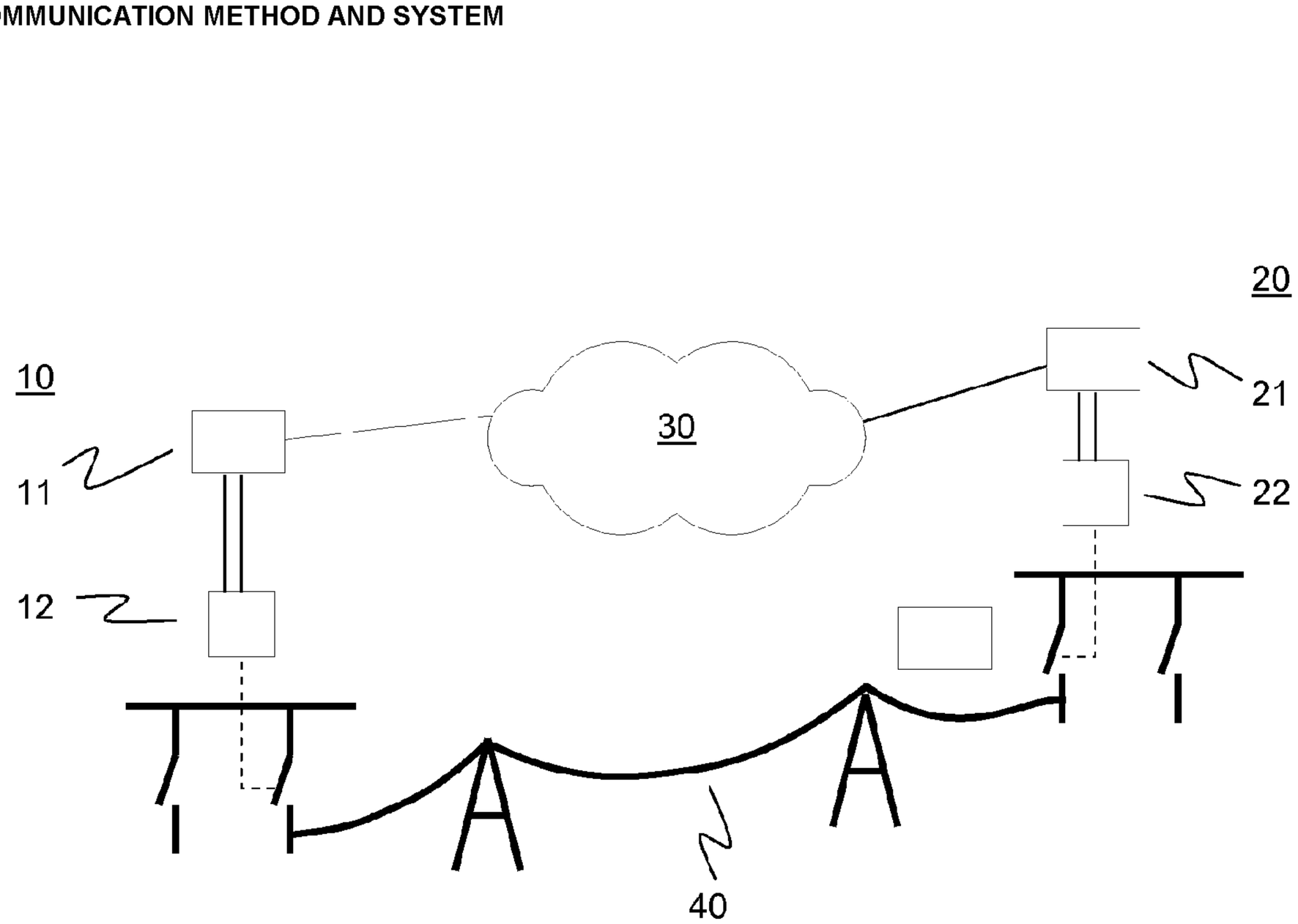
(51) **Cl.Int./Int.Cl.** ***H04B 3/54*** (2006.01),
H04B 15/00 (2006.01)

(72) **Inventeurs/Inventors:**
WIMMER, WOLFGANG, CH;
KIRRMANN, HUBERT, CH;
SPIESS, HERMANN, CH;
RAMSEIER, STEFAN, CH;
NOTTER, ALLEN, CH;
ISRAEL, MARTIN, CH

(73) **Propriétaire/Owner:**
ABB TECHNOLOGY AG, CH

(74) **Agent:** NORTON ROSE FULBRIGHT CANADA LLP/S.E.N.C.R.L., S.R.L.

(54) **Titre : PROCEDE ET SYSTEME DE COMMUNICATION**
(54) **Title: COMMUNICATION METHOD AND SYSTEM**



(57) **Abrégé/Abstract:**
The present invention increases reliability of communication over a non- deterministic communication channel, and is particularly suited for inter-substation teleprotection in electric power systems. A communication channel is being monitored based on regular network traffic, i.e. by evaluating messages or data packets carrying real-time operational data as a payload. A permanent determination of a channel quality, including appropriate alarming in case the channel quality is found insufficient, is based on an evaluation, at a receiving node, of data packets continually transmitted by a sending node. These continually or repeatedly transmitted data packets may comprise identical payloads reflecting current states rather than state changes as operational data.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 July 2010 (22.07.2010)

PCT

(10) International Publication Number
WO 2010/081798 A1

(51) International Patent Classification:
H04B 3/54 (2006.01) *H04B 15/00* (2006.01)

(21) International Application Number:
PCT/EP2010/050273

(22) International Filing Date:
12 January 2010 (12.01.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09150630.3 15 January 2009 (15.01.2009) EP

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

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WIMMER, Wolfgang** [DE/CH]; Hinterdorf 220, CH-5323 Rietheim (CH). **KIRRMANN, Hubert** [FR/CH]; Im Rütli 17, CH-5404 Dättwil (CH). **SPIESS, Hermann** [CH/DE]; Dorfstrasse 129, CH-5245 Habsburg (CH). **RAMSEIER, Stefan** [CH/CH]; Sonnmattweg 14, CH-5416 Kirchdorf (CH). **NOTTER, Allen** [CH/CH]; Zelgmatte 5, CH-5600 Lenzburg (CH). **ISRAEL, Martin** [DE/CH]; Sattlermattstrasse 16, CH-4535 Hubersdorf (CH).

(74) Agent: **ABB Patent Attorneys**; c/o ABB Schweiz AG, Intellectual Property (CH-LC/IP), Brown Boveri Strasse 6, CH-5400 Baden (CH).

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

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

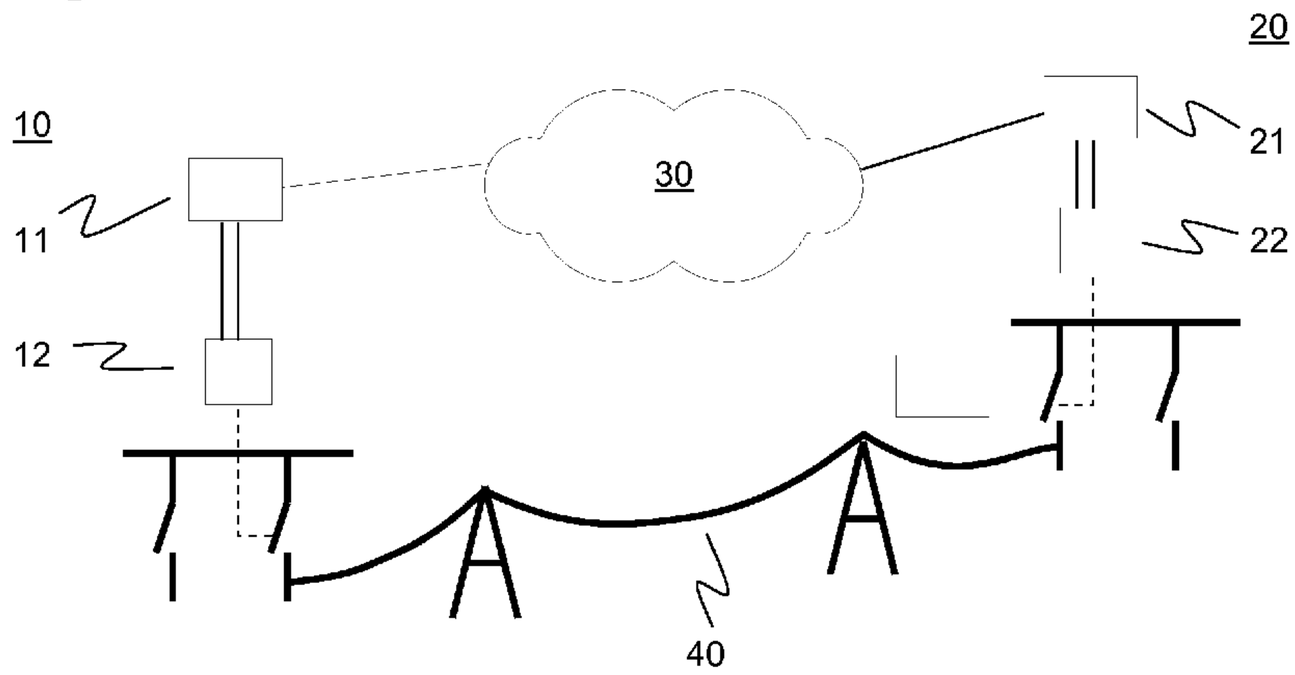
Published:

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

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

(54) **Title**: COMMUNICATION METHOD AND SYSTEM

Fig. 1



(57) **Abstract**: The present invention increases reliability of communication over a non-deterministic communication channel, and is particularly suited for inter-substation teleprotection in electric power systems. A communication channel is being monitored based on regular network traffic, i.e. by evaluating messages or data packets carrying real-time operational data as a payload. A permanent determination of a channel quality, including appropriate alarming in case the channel quality is found insufficient, is based on an evaluation, at a receiving node, of data packets continually transmitted by a sending node. These continually or repeatedly transmitted data packets may comprise identical payloads reflecting current states rather than state changes as operational data.

WO 2010/081798 A1

DESCRIPTION

COMMUNICATION METHOD AND SYSTEM

FIELD OF THE INVENTION

The invention relates to the field of utility communication, and in particular to communication of real-time operational data between distant sites of an electric power utility enterprise. It departs from a communication method as described in the preamble of claim 1.

BACKGROUND OF THE INVENTION

Electric power utilities or transmission system operators own and operate electric power transmission networks interconnecting sites, such as power sources and substations, which despite being distant from each other some 100 km or more, have to be coordinated in one way or the other. Across their utility communication systems, a variety of messages are transferred over long distance communication links between distant sites of the utility in order to safely transmit and distribute electric energy. For some of these messages, and in particular for teleprotection commands, the transmission delay between transmitter and receiver is critical and should not exceed a few milliseconds up to some 10 ms.

Dedicated remote tripping devices or protection signal transmission devices, also known as teleprotection devices, are generally used for transmitting protection or switching commands for distance and differential protection schemes in electrical high-voltage and medium-voltage networks and systems. Protection commands result, for example, in a circuit breaker being opened directly or indirectly and, in consequence in electrical disconnection of a selected part of the network or of the system. Conversely, other protection commands result in the opening of a circuit breaker in the remote station being prevented or blocked. In order for a protection command to be transmitted from one point of a power transmission or distribution network to another, a transmitter in a remote tripping device produces signals in accordance with the protection command, which are transmitted via a physical signal link. A receiver in another remote tripping device detects

the transmitted signals and determines the corresponding number and nature of the protection commands. The physical signal link may involve radio waves or fiber optics, but preferably, the protection signals are transmitted over pilot wires, analog leased lines, voice channels of analog or digital communication systems, or even high-voltage electricity transmission lines, the latter being known as power line communication (PLC).

US 2003/081634 A1 is concerned with conventional audio tone teleprotection via a dedicated audio telecommunication link between two substations, and including time division multiplexed frames being transmitted continuously from a sender to a receiver in a deterministic manner. At the sender, a special framing pattern (pre-selected pattern of 8 bits) is inserted in the last timeslot of each frame, thus decreasing bandwidth available for operational data. If the known framing pattern is not detected repeatedly at the receiver override information signals are inserted into the de-framed data stream to prevent a noise signal from producing a false output state.

For transmitting messages over long distances from one site to the other, the utility may rely on public or proprietary communication networks with non-deterministic behaviour. In this context, a Wide-Area communication Network (WAN) designates a packet switched communication network interconnecting two sites of the utility, and comprising a number of IP networks with specific network elements such as routers, switches, repeaters and possibly optical transmission media at the physical layer. WANs are in general very reliable, however said network elements may cause irregular network delays, occasional bit errors and inherent link failures, which all contribute to a non-deterministic behaviour of the network. In packet switched networks with individual data packets carrying destination addresses, heavy load on a communication channel or a specific network element may lead to increased delay or packet loss, whereas link failure can cause delays due to reconfiguration of the routers.

For time-critical applications, increased delay or packet loss may result in a malfunction of a system. For an electric power utility, in the worst case, substantial damage can occur to a substation if a trip signal is delayed. WANs can also be target of unlikely, but potentially harmful acts of intrusion comprising e.g. inserting intentionally wrong commands at one of the routers. As a consequence, any communication channel involving a WAN may be considered both non-deterministic, or non-synchronous, and non-secure. Use of non-deterministic communications for command and control means that one can not guarantee delivery nor the actual communication path taken by a packet. Specifically, the

use of the Internet increases the risk of critical control system communications failure, as attacks against other entities could greatly impact any control communications that uses this path or shares resources that touch the Internet.

Conventionally, dedicated teleprotection systems monitor the state and delay of a communication system by means of dedicated loop test messages that operate as follows: two stations, A and B, are connected via a communication link. Station A transmits a special message to station B, which receives it and immediately sends back an “echo” to station A. When station A receives this “echo”, it knows that the communication link is working, and it can also measure the transmission delay (half the time it takes the loop test message to travel from A to B and back to A). A loop test messages is typically sent once every few hours, accordingly, changes of the transmission delay in real-time can not be detected.

Alternatively, the delay measurement method specified in IEEE 1588 (IEEE Standard 1588-2002, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, aka Precision Time Protocol PTP) can be used in order to monitor a state and/or availability of a communication system. Standard two-way time synchronisation protocols such as IEEE 1588 define methods for synchronising devices via a communication network such as a Local Area Network (LAN), to a high precision (better than one microsecond).

In the field of Voice over IP (VoIP), voice calls are routed over an Internet Protocol (IP) network, and a Quality of Service (QoS) is an important issue between the service provider and the end user. In this context, and more generally for the purpose of real-time data transmission, the Real-Time Protocol (RTP) within the ISO-OSI layer reference model prescribes the encapsulation of e.g. encoded voice data in RTP packets. The latter are passed to the transport layer and further to the Internet Protocol (IP) network layer. At the transport layer, data transmission systems may use either a reliable protocol (such as a Transmission Control Protocol TCP) or an unreliable protocol (such as User Datagram Protocol UDP). The former ensures that all the packets arrive at the receiver, but requires more bandwidth due to protocol overhead and it introduces more delay. The reliable transport protocols normally measure the round-trip delay in order to derive there from

when messages should be repeated. On the other hand, unreliable protocols are lightweight and faster although the data stream may be subject to packet loss.

In the patent application US 2007/0230361 A1, a method is provided for monitoring a packet-switched network via which real time VoIP data is transmitted. Data packets containing real-time data are sniffed in order to monitor a QoS parameter. The QoS parameter comprises one of egress delay, ingress delay, jitter, roundtrip delay, packet loss, throughput, instantaneous signal loss, and accumulated content loss. In another patent application US 2002/105909 related to VoIP, as long as the smoothing algorithm that adjusts for transitory effects while evaluating packet loss data yields acceptable values, calls continue to be routed over the IP network. If, on the other hand, the value exceeds a threshold, a QoS Monitor blocks routing over the IP network and routes calls over an alternative network, such as a Switched Circuit Network (SCN).

DESCRIPTION OF THE INVENTION

It is therefore an objective of the invention to enable a utility, in particular an electric power utility, to make efficient use of non-deterministic communication channels for exchanging real-time operational data between distant sites of the utility. This objective is achieved by a communication method and a communication system according to the claims 1 and 10. Further preferred embodiments are evident from the dependent patent claims.

According to the invention, a non-deterministic communication channel comprising a Wide Area Network (WAN) with packet switched communication, such as e.g. an Internet Protocol (IP) network, is being monitored based on regular network traffic, i.e. by evaluating continually sent data packets carrying real-time operational data as a payload. Hence, no permanent occupation of bandwidth in a deterministic communication channel is required, nor is there any additional overhead network traffic in the form of test messages or message duplicates generated on the non-deterministic channel, and a minimum usage of, or interference with, the communication channel is achieved. A permanent determination and monitoring of a channel quality, including appropriate alarming in case the channel quality is found insufficient, is based on an evaluation, at a receiving node, of data packets continually transmitted by a sending node. These continually or repeatedly transmitted data packets may comprise, as operational data, identical payloads reflecting current states rather than state changes. Ultimately, the

reliability of a communication over a non-deterministic channel without message confirmation is increased.

The communication method is most beneficially used in an electric power system, where the data packets comprise protection commands to protect a power line between two sites of the electric power system, and where a site is a power source, a power sink, or a substation. The protection of the power line may be a distance or differential protection scheme, and result e.g. in a blocking, unblocking, or permissive state of a switching device at the remote site. The repeatedly transmitted data packets may be seen as replacing a conventional guard signal in conventional teleprotection channels.

In a preferred variant, the receiving node determines channel availability as a binary and rapidly updatable channel quality measure. To this purpose, the receiving node verifies whether data packets with the expected type of payload are actually received, and whether the delay in-between successively received data packets is in the expected range. If the time elapsed between successive data packets exceeds a certain threshold, the channel availability is, at least temporarily, considered insufficient. Appropriate measures are then taken at the receiving node, such as alarm generation, conversion to a stand-alone or island operation mode, or, in case a signal is deemed missing, a switching device at the second site being unblocked.

In an advantageous embodiment, the proposed protocol for payload transmission and channel supervision comprises including, in the data packets, a send sequence number. Send sequence numbers are preferred over time stamps because of possible irregularities in the time source at the sender due to e.g. clock synchronisation, manual time setting or daylight savings time. By proper monitoring of the sequence numbers, several types of channel errors can be detected and logged, such as packet loss, packet duplication and reception of packets in the wrong order, i.e. not in the order in which they had been dispatched. All these errors point to a degrading channel quality in the WAN.

In a further variant, the data packet comprises a response request flag. If the latter is set, a response message is prepared by a destination node of the original data packet and immediately returned to the source or originating node. The response message comprises the received “send sequence number”. By measuring the elapsed time between the transmission of a response request and the reception of a response message as identified by the same send sequence number, the source node can estimate a round trip delay or time of the communication channel. If this permanent response time measurement then detects a

delay that exceeds a configurable threshold, an alarm is generated informing the user that the quality of the non-deterministic communication channel is no longer guaranteed, and that a different communication channel should be chosen, or that the message contents should be temporarily ignored.

In a further preferred embodiment, the sending node is connected to a relay at the first site or substation, and permanently transmitting a state received from the latter. In the event of a changed state or signal being input to the node, and in order to convey the new information as fast as possible, the repetition rate or transmit frequency of the data packets carrying the new state is increased, at least temporarily. For instance, N = 16 repeats at an increased rate of one message every 2 ms are generated, before returning to a standard rate of one maintenance message every 5 ms.

Finally, cyber security aspects of the proposed transmission over non-secure communication channels is taken care of by a hash or message digest that is transmitted as part of the data packet and calculated on the basis of the header and payload fields. The hash enables to verify the authenticity of the data packet, and thus provides, if needed in combination with the sequence number and node address, for a basic protection against various security threats.

Preferably, the proposed protocol is implemented in a peer-to-peer fashion in both communication nodes, such that each node can independently measure the channel quality and signal alarms.

BRIEF DESCRIPTION OF THE DRAWINGS

The subject matter of the invention will be explained in more detail in the following text with reference to preferred exemplary embodiments which are illustrated in the attached drawings, in which:

Fig.1 schematically depicts a utility communication network,

Fig.2 is an excerpt of an exemplary data packet, and

Fig.3 schematically shows a sequence of maintenance packets and one response packet.

The reference symbols used in the drawings, and their meanings, are listed in summary form in the list of reference symbols. In principle, identical parts are provided with the same reference symbols in the figures.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Fig.1 depicts a utility communication network with a first node or terminal 11, a second node or terminal 21, and a Wide Area Network (WAN) 30 as part of a non-deterministic communication channel, e.g. based on User Datagram Protocol (UDP) with unacknowledged transmission between the two nodes. The two nodes 11, 21 are dedicated teleprotection devices located at a first substation 10 and at a second substation 20, respectively, and hardwired to a number of protection relays 12, 22 or other secondary equipment of the respective substation. The two nodes 11, 21 may be interconnected via other communication channels, such as a Power Line Communication (PLC) channel along an overhead power line 40 between the two substations 10, 20. The relays 12, 22 in turn are connected to the primary equipment of the substation and provide a signal or state to be transmitted, e.g. a tripping signal or command related to a distance protection function of the overhead power line 40.

Fig.2 shows an excerpt of an exemplary data packet 50 to be sent, by the first node 11, across the non-deterministic communication channel 30 to the second node 21. The data packet comprises a header, payload and trailer as part of a teleprotection application layer. The header includes, among other fields, special header fields with a Response-Request flag 51, a teleprotection Node Address 52, and a send sequence number 53. The payload field 54 comprises one or several signals or protection commands in the form of a relatively short bit sequence. It is followed by a first trailer field with a message digest or hash 55 calculated on the basis of the header and payload fields. The hash provides for a basic protection against, and enables, if needed in combination with the sequence number 53 and node address 52, detection of various security threats, e.g. unauthorized (faked) messages, wrong partner, man-in-the-middle, or message replay. Further trailer fields may follow, such as a retransmission count 56 that is incremented in case of a retransmission, at an increased repetition rate and following a particular event, of otherwise unchanged data packets with identical sequence number and hash. The application layer data is embedded in headers and trailers according to the OSI transport (UDP) network (IP) and physical (Ethernet) layers (not shown in Fig.2).

Fig.3 shows an exemplary sequence of messages 50, 50', 50" exchanged between nodes 11 and 21, where time is progressing from top to bottom, and where each diagonal represents a single message. The first node 11 continually sends data packets at regular intervals separated by idle periods with no sending activity, e.g. every 5 ms. The data

packets are received by the second node 21, and as long as the messages are received in order, and/or with the expected inter-message delays Δt, the channel 30 is assumed to be available, and the payload conveyed by the messages is duly evaluated at the receiving end. Occasionally, the response request flag 54 in the data packet 50" is set, upon which the second node responds with a response message 60. The reception of the latter at the first node, and in particular a round trip time delay comprising the cumulated transmission times, or delays, of the response-requesting data packet 50" and the response message 60, in turn can be evaluated in view of a channel quality. The response requests are sent periodically, but at a much lower rate (e.g. every 100 ms to 10 sec) than the data packets without response request.

LIST OF DESIGNATIONS

10, 20 substation
11, 21 node
12, 22 relay
30 WAN
40 power line
50 data packet
51 response request flag
52 node address
53 sequence number
54 payload
55 hash
56 retransmission count
60 response message

PATENT CLAIMS

1. A method of communicating between a first communication node (11) at a first site (10) and a second communication node (21) at a second site (20), comprising
- sending, by the first node (11), a message comprising operational data (54) over a communication channel (30) to the second node (21), and monitoring a channel quality of the communication channel (30) based on the message,
characterized in that the method comprises
- sending continually, by the first node (11), data packets (50, 50', 50") comprising operational data (54) over a non-deterministic communication channel (30) comprising a packet-switched network to the second node (21), and
- monitoring, by the second node (21) and based on said data packets (50, 50', 50"), the channel quality.

2. The method according to claim 1, wherein the two sites (10, 20) are connected via a power line (40) of an electric power transmission network, characterized in that the method comprises
- continually sending data packets (50, 50', 50") comprising operational data in the form of protection commands for the power line (40).

3. The method according to claim 1 or 2, wherein the first node (11) is adapted to receive a protection command as an input signal from a relay (12) connected to the first node (11), characterized in that the method comprises
- increasing, as soon as the input signal from the relay changes, a repetition rate of the continually sent data packets (50, 50', 50").

4. The method according to claim 1 or 2, comprising
- determining, by the second node (21), a channel availability based on an expected and an observed reception of data packets (50, 50', 50").

5. The method according to claim 4, comprising
- determining the channel availability based on an inter-message time delay Δt between two successively sent data packets (50, 50').

6. The method according to claim 4, wherein the data packets (50, 50', 50") comprise a send sequence number (53), characterized in that the method comprises
- determining the channel availability based on the send sequence numbers (53) of the received data packets.

7. The method according to claim 1 or 2, wherein the data packets (50) comprise a response request flag (51), characterized in that the method comprises
- responding, by the second node (21) and if the response request flag (51) of a received data packet (50") is set, with a response message (60), and
- determining, by the first node (11), a channel quality based on the response message (60).

8. The method according to claim 7, comprising
- determining the channel quality based on a round trip time delay of the data packet with the response request flag (51) being set and the response message (60).

9. The method according to claim 1 or 2, wherein the data packets (50) comprise a hash (55), characterized in that the method comprises
- determining, by the second node (21) and based on the hash (55), whether the data packet (50) is authentic.

10. A communication system with a first node (11), a second node (21), and a non-deterministic communication channel (30), adapted to perform a communication method according to any one of claims 1 to 9.

11. A method of communicating between a first communication node at a first site and a second communication node at a second site, comprising
- sending, by the first communication node and continually at regular intervals separated by idle periods with no sending activity, data packets including operational data over a non-deterministic communication channel including a packet-switched network to the second communication node, and
- monitoring, by the second communication node and based on said data packets, the channel quality.

Fig. 1

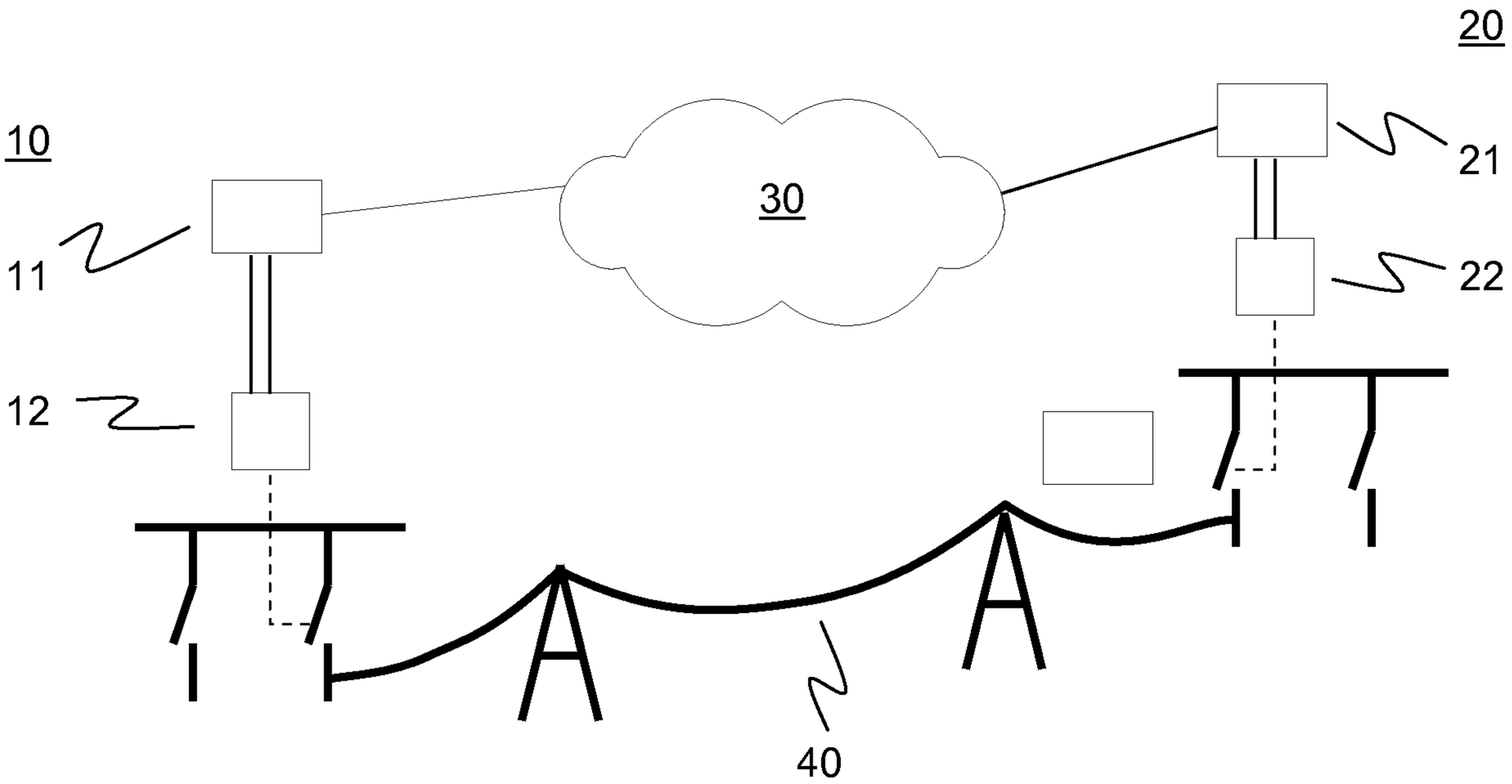


Fig. 2

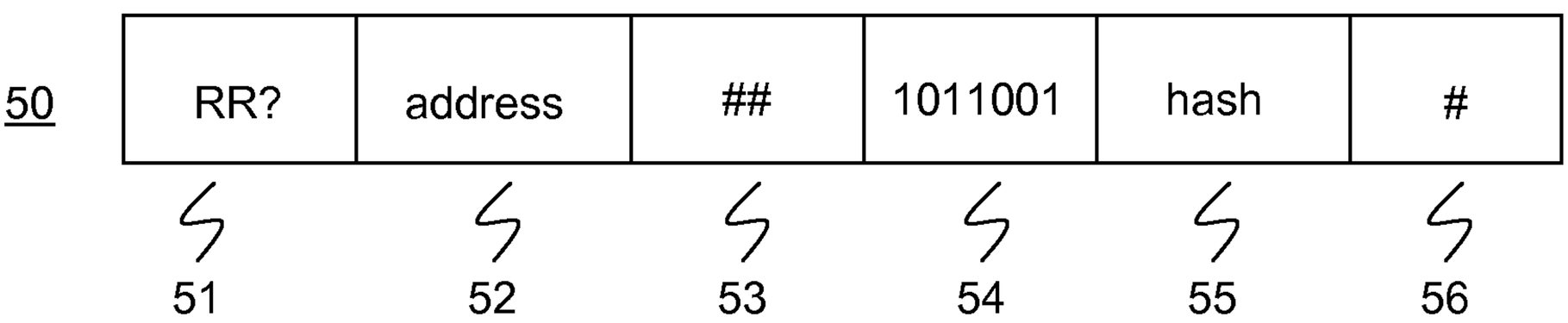
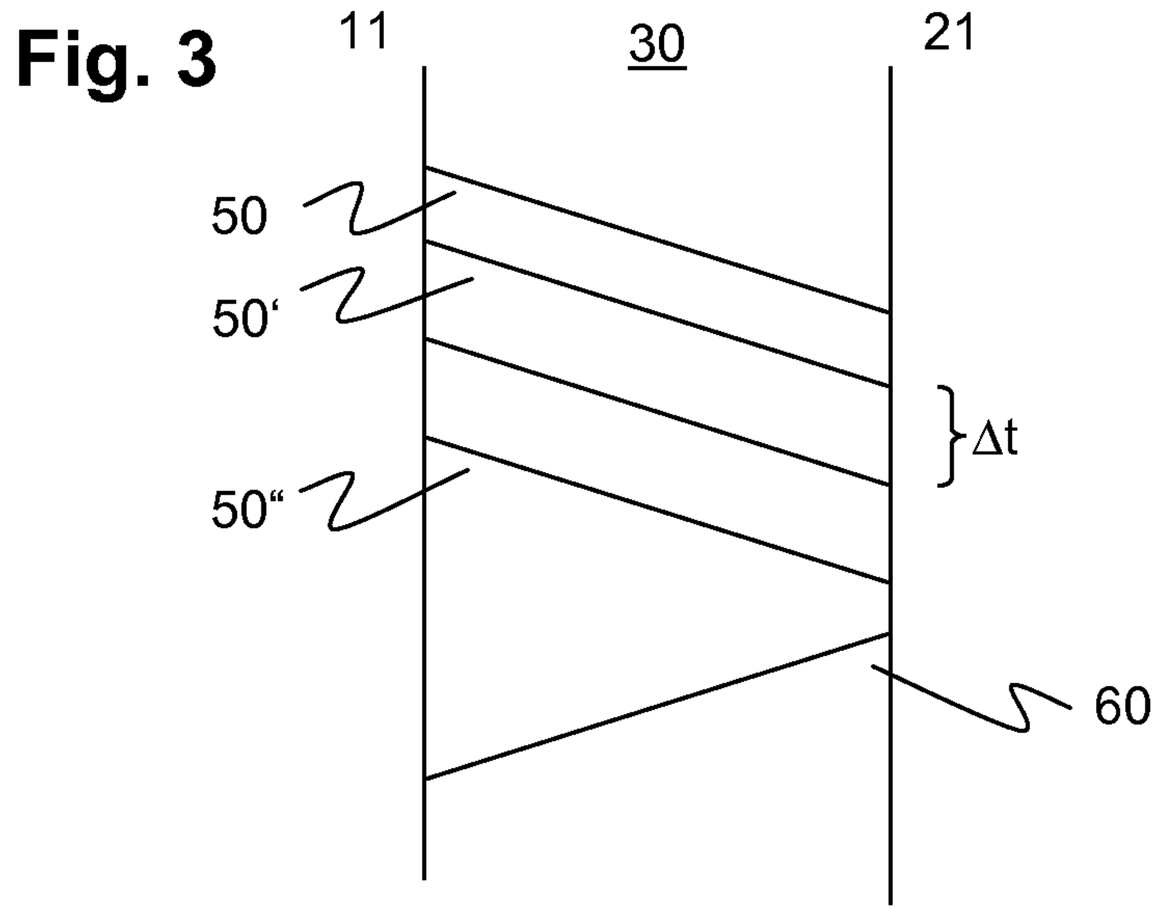
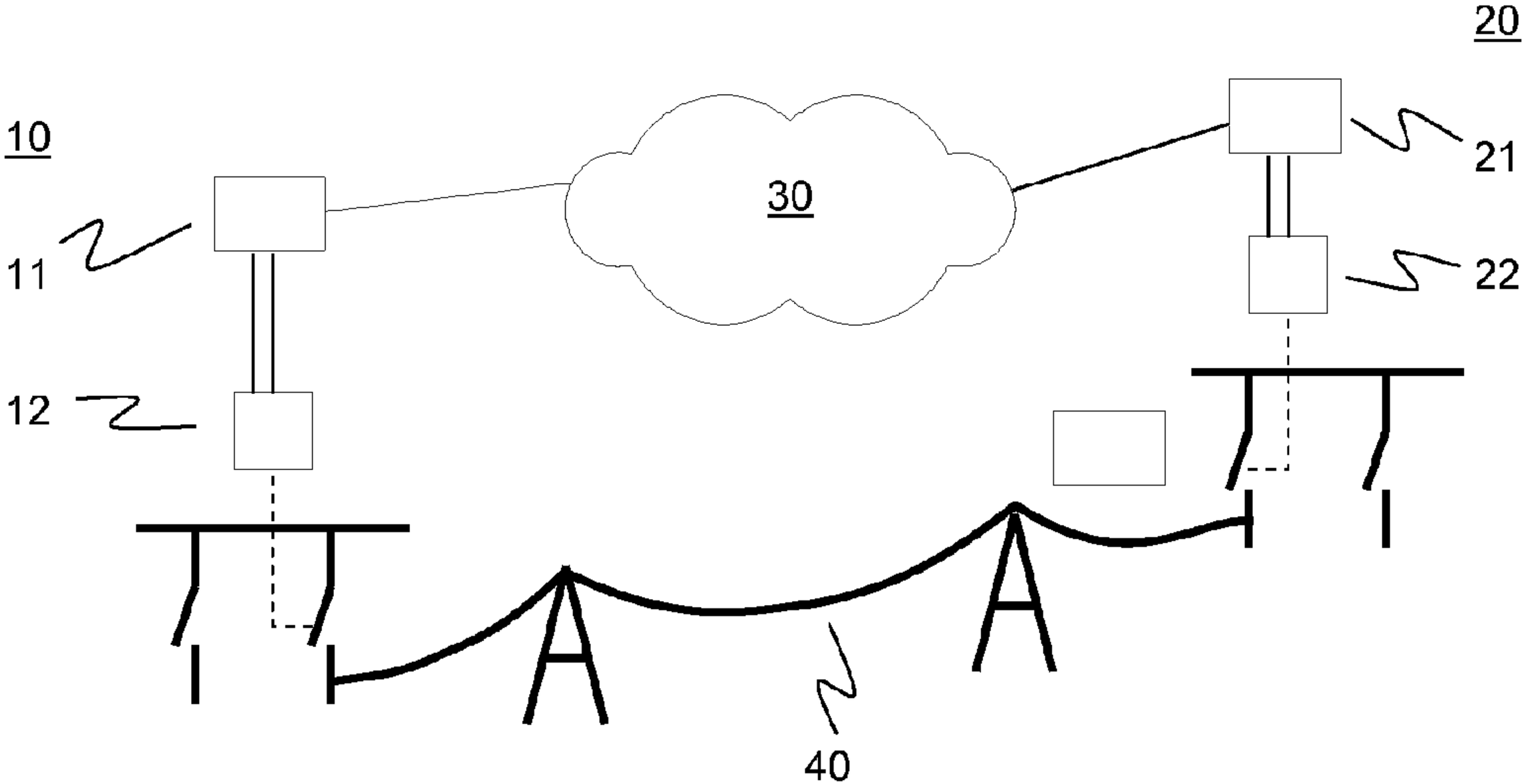


Fig. 3




10
11
12
30
20
21
22
40