



(86) Date de dépôt PCT/PCT Filing Date: 2013/12/20
(87) Date publication PCT/PCT Publication Date: 2014/06/26
(85) Entrée phase nationale/National Entry: 2015/06/18
(86) N° demande PCT/PCT Application No.: SE 2013/051595
(87) N° publication PCT/PCT Publication No.: 2014/098760
(30) Priorités/Priorities: 2012/12/21 (US61/740,712);
2012/12/21 (SE1251511-0)

(51) Cl.Int./Int.Cl. *E05B 47/00* (2006.01),
B25F 5/00 (2006.01), *E05B 49/00* (2006.01),
E05B 73/00 (2006.01), *G07C 9/00* (2006.01)
(71) Demandeur/Applicant:
NIDA TECH SWEDEN AB, SE
(72) Inventeur/Inventor:
DACKEFJORD, HAKAN, SE
(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : PROCEDE, NOEUD, PROGRAMME INFORMATIQUE ET SYSTEME D'OUTIL A COMMANDE MECANIQUE
PERMETTANT DE VERROUILLER ET DE DEVERROUILLER UN OUTIL A COMMANDE MECANIQUE
(54) Title: METHOD FOR AND TOOL LOCK

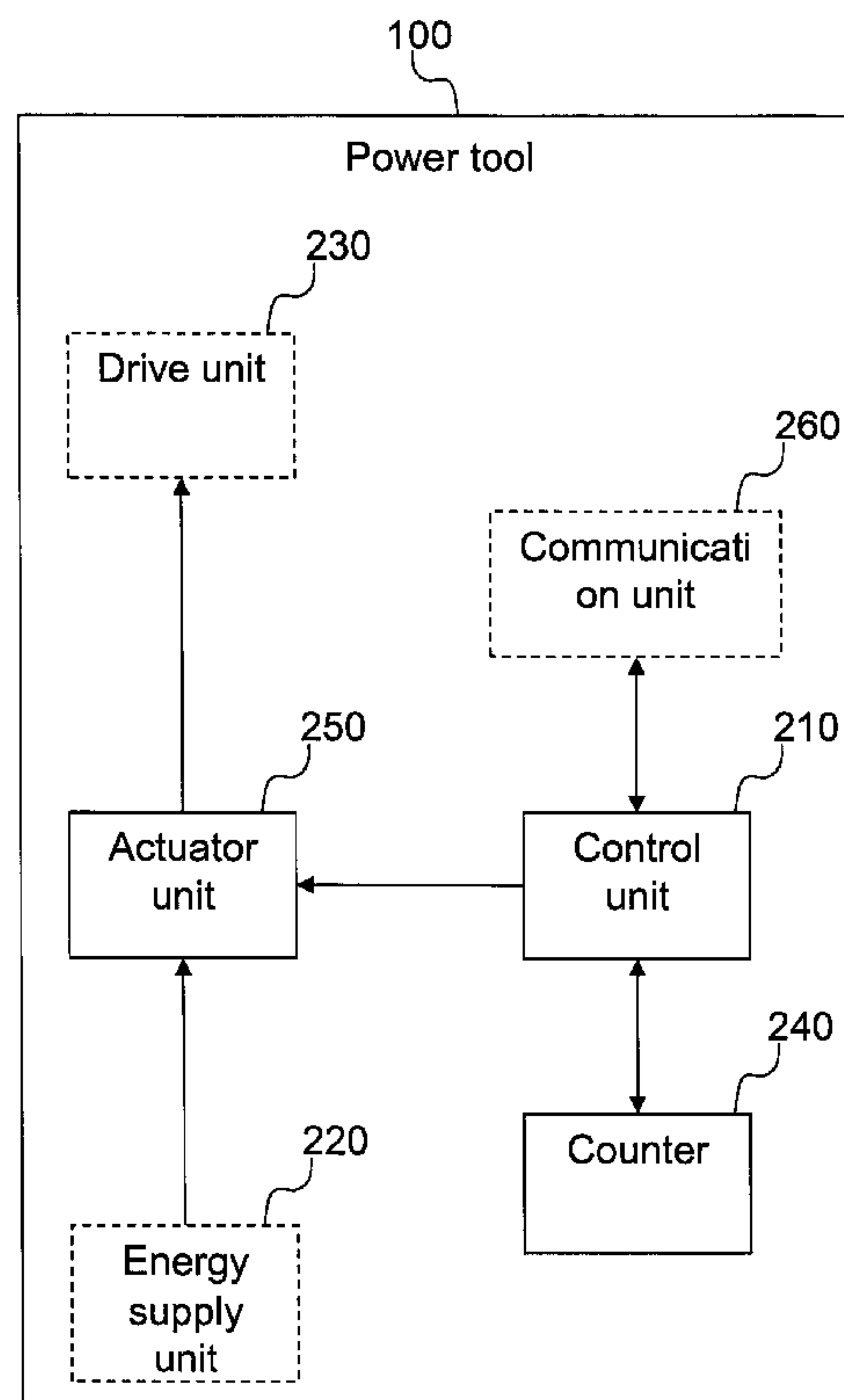


Fig. 2

(57) Abrégé/Abstract:

Methods, nodes, a power tool and computer programs for and in a power tool (100) for enabling unlocking and locking of the power tool for prevention of unauthorized use, the method comprising receiving (S100) an unlock message to a control unit (210),



(57) Abrégé(suite)/Abstract(continued):

the message including an instruction to unlock the tool (100), unlocking (S110) the power tool (100) according to the instruction by the control unit (210) via an actuator unit (250), counting (S120) an authorization time period from reception of the first message to the control unit (210) by a counter (230), wherein when the counted authorization time period exceed a predetermined threshold, locking (S130) the power tool (100) by the control unit (210) via the actuator unit (250), thereby enabling prevention of unauthorized use of the power tool (100) by remote unlocking and locking.

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

(19) World Intellectual Property
Organization
International Bureau



(10) International Publication Number
WO 2014/098760 A1

(43) International Publication Date
26 June 2014 (26.06.2014)

(51) International Patent Classification:

E05B 47/00 (2006.01) *E05B 73/00* (2006.01)
B25F 5/00 (2006.01) *G07C 9/00* (2006.01)
E05B 49/00 (2006.01)

(21) International Application Number:

PCT/SE2013/051595

(22) International Filing Date:

20 December 2013 (20.12.2013)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

1251511-0 21 December 2012 (21.12.2012) SE
61/740,712 21 December 2012 (21.12.2012) US

(71) Applicant: **NIDA TECH SWEDEN AB** [SE/SE]; By-
hornsgränd 8, S-216 23 Malmö (SE).

(72) Inventor: **DACKEFJORD, Håkan**; Långsjövägen 107, S-
125 51 Älvsjö (SE).

(74) Agent: **BERGENSTRÄHLE & LINDVALL AB**; Box
17704, S-118 93 Stockholm (SE).

(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, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: METHOD, NODE, COMPUTER PROGRAM AND POWER TOOL DEVICE, FOR ENABLING LOCKING AND UN-
LOCKING OF POWER TOOL

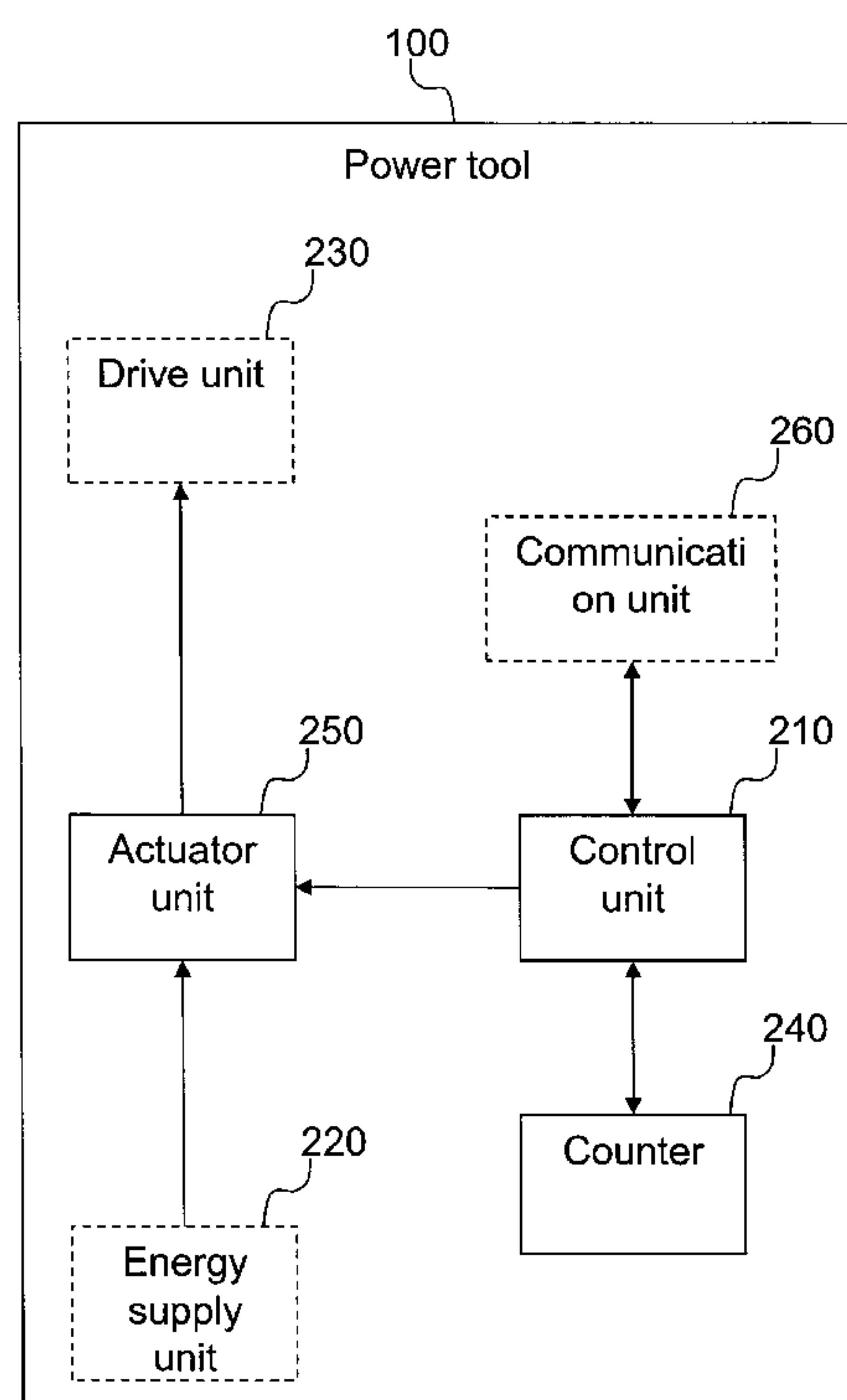


Fig. 2

(57) Abstract: Methods, nodes, a power tool and computer programs for and in a power tool (100) for enabling unlocking and locking of the power tool for prevention of unauthorized use, the method comprising receiving (S100) an unlock message to a control unit (210), the message including an instruction to unlock the tool (100), unlocking (S110) the power tool (100) according to the instruction by the control unit (210) via an actuator unit (250), counting (S120) an authorization time period from reception of the first message to the control unit (210) by a counter (230), wherein when the counted authorization time period exceed a pre-determined threshold, locking (S130) the power tool (100) by the control unit (210) via the actuator unit (250), thereby enabling prevention of unauthorized use of the power tool (100) by remote unlocking and locking.

WO 2014/098760 A1

WO 2014/098760 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, — *before the expiration of the time limit for amending the*
KM, ML, MR, NE, SN, TD, TG). *claims and to be republished in the event of receipt of*
Published: *amendments (Rule 48.2(h))*
— *with international search report (Art. 21(3))*

The Swedish Patent Office
PCT International Application

1

PCT/SE2013/051595
27-01-2015

METHOD FOR AND TOOL LOCK

Technical field

[0001] The present disclosure relates generally to methods, nodes, computer programs and a power tool for enabling unlocking and locking of the power tool for prevention of unauthorized use.

Background

[0002] Entrepreneurs and construction companies are using various machines and tools on construction sites. This ranges from the self-employed carpenter performing a renovation of a cottage all the way to the large construction company building entire new hospitals, districts, highways, bridges and other major projects. The workers doing the construction uses all kind of tools from pencils and knives all the way to excavators and cranes. When it comes to power tools, also frequently used by the construction workers, they may involve a significant value in combination with a compact format. Such tools may include electric driven tools, fuel/gasoline driven tools, pneumatic driven tools, hydraulic driven tools, not limiting to similar powered tools. Examples of power tools are: screwdrivers, bolt gun, nail gun, impact drill, angle grinder, cutter, saw, reciprocating saw, not limiting to other types of tools. Obviously a crane may represent a large capital value, but it is rather unpractical for the simple thief or the regular criminal organization to steal a crane. However, the power tool is easy to carry away and may represent a significant value on a market, or may be used for other criminal activities. This is a vast problem for construction companies, which power tools is being stolen or just disappears from construction sites. The lost tools costs money to replace drives insurance costs, and delays planned work.

[0003] Another problem is where owner of tools, for example tool rental companies, is to get rental returns of tools in time or according to an agreement.

AMENDED SHEET

[0004] Another problem, of a rather practical character, which yet may be troublesome, may be on a large construction site, to find tools being spread out over a large area or space.

[0005] US20120234058A1 describes a wireless access control system including a remote access device. A plugin device communicates with the remote access device and a lock controls the ability to lock and unlock a door in which the lock is disposed. The plugin device determines a distance between the remote access device and the lock and causes the lock to communicate with the remote access device when the remote access device is at a distance less than or equal to a predetermined distance from the lock to enable the lock to be unlocked.

[0006] US20110289123A1 describes a method for controlling and recording the security of an enclosure. A mobile electronic control device such as an electronic key, is used to access or otherwise control the operations of a field device, such as an appliance, power tool, shipping container, and the like. In a control event in which the mobile control device interacts with the field device via wired or wireless communications, the control device obtains the current location and the field device ID. The communications between the mobile control device and the field device may be secured with encryption. The location information is used by the mobile control device to determine whether the field device should be accessed or enabled. Alternatively, the location information may be stored separately in a location sensing device, and the control event data recorded by the key and the location information recorded by the location sensing device are later combined when they are downloaded into a management system for auditing.

[0007] US6469615B1 describes an operating control device can be use on equipment such as hand tools, electronics or fuel pumps. An input device enables the input of user access codes and a readout panel monitors the equipment status. A control member is in communication with the input device, readout panel, power source, driver member and activation member to prevent operation of the equipment by requiring entry of a user code. The control device can include a

programmable timer to communicate with the control member to enable the power to flow from the power source to the driver member for a predetermined period of time. A clock can track time and activate and deactivate the timer. The communication can be through electrical wires that can be encased in a solid material to make the control member and wires inaccessible. When used directly on a fuel pump, the control member prevents fuel from reaching the engine without the input of a proper user code. Alternatively, the control device can be a fuel line shutoff valve to prevent fuel from traveling along the line. A solenoid can be used in the shutoff valve to prevent flow of fuel from the gas tank to the driver.

[0008] WO2006021047A1 describes an access control system for two door access points that are selectively accessed by a plurality of users. The system includes access tokens for respective users having memory for containing a digital certificate and a token certificate change list. Each token is responsive to an interrogation signal for generating a token signal derived from the certificate. A computer network contains information indicative of the certificates for the system, and allows system to provide a central that is indicative of changes that are required to one or more of those certificates. A connected access reader is disposed adjacent to access point and communicates with network for maintaining a first local that is merged in real time with the central. Reader generates an interrogation signal and is responsive to the corresponding token signal for determining if access point is to be pulsed to the unlocked configuration.

Summary

[0009] It is an object of the invention to address at least some of the problems and issues outlined above. It is possible to achieve these objects and others by using a method and an apparatus as defined in the attached independent claims.

[00010] According to one aspect, a method is provided in a power tool for enabling unlocking and locking of the power tool for prevention of unauthorized use, the method comprising: receiving an unlock message to a control unit, the message including an instruction to unlock the tool, unlocking the power tool

according to the instruction by the control unit via an actuator unit, counting an authorization time period from reception of the first message to the control unit by a counter, wherein when the counted authorization time period exceed a predetermined threshold, locking the power tool by the control unit via the actuator unit, thereby enabling prevention of unauthorized use of the power tool by remote unlocking and locking.

[00011] According to another aspect, a method is provided in a tool control node for enabling unlocking and locking of a tool for prevention of unauthorized use, the method comprising transmitting an unlock message to the tool, the message including an instruction to unlock the tool, counting an authorization time period from transmission of the unlock message to the tool, wherein when the counted authorization time period exceed a predetermined threshold, transmitting of a lock message including an instruction to lock the tool, thereby enabling prevention of unauthorized use of the tool by remote unlocking and locking.

[00012] According to another aspect, a power tool is provided adopted to enable unlocking and locking of the power tool for prevention of unauthorized use, the power tool adopted to receive an unlock message to a control unit, the message including an instruction to unlock the tool, unlock the power tool according to the instruction by the control unit via an actuator unit, count an authorization time period from reception of the first message to the control unit by a counter, wherein when the counted authorization time period exceed a predetermined threshold, lock the power tool by the control unit via the actuator unit, thereby enabling prevention of unauthorized use of the power tool by remote unlocking and locking.

[00013] The above methods, tool control node and power tool may be configured and implemented according to different optional embodiments. In one possible embodiment, the actuator unit is at least one of electrical switch, mechanical lock and semiconductor based switch. In another possible embodiment when a second unlock message is received before the predetermined

threshold is reached, the counter is restarted, such that the power tool remains unlocked. In another possible embodiment the unlock message includes a first key, wherein, the first key is required by the control unit for authorization of the message. In another possible embodiment the drive unit requires at least one of the first key or a second key from the control unit, for enabling of the drive unit. In another possible embodiment a lock message is received by the control unit, the lock message including an instruction to lock the tool, wherein the tool is locked by the control unit via the actuator unit. In another possible embodiment a position message including an alert signal is received by the control unit, the position message including an instruction to repeatedly transmit a response signal as a response to the alert signal, thereby enabling positioning of the tool. In another possible embodiment the communication with the tool is encrypted. In another possible embodiment the tool has a physical tamper protection.

[00014] In another embodiment the positioning of the tool is instead made by the tool control unit. This could for example be done through means of a message including an alert signal is received by the control unit. The message triggers the control unit to transmit a signal requesting response signals from presence nodes nearby followed by receiving response signals to the control unit from presence nodes nearby and thereby enabling positioning of the tool. This allows for the positioning to in one embodiment be made within the tool enabling for the tool to send a response comprising a position to for example the tool control node.

[00015] In another embodiment a power tool control unit adopted to enable unlocking and locking of a tool for prevention of unauthorized use is adopted to:

- transmit an unlock message to the tool, the message including an instruction to unlock the tool,
- determine the position of the tool and check if said tool is within a predetermined area,

- if the tool leave said predetermined area transmit a lock message including an instruction to lock the tool, thereby enabling prevention of unauthorized use of the tool.

[00016] The power tool control unit can further be configured to sound and transmit an alarm if said tool leaves the predetermined area.

[00017] Further possible features and benefits of this solution will become apparent from the detailed description below.

Brief description of drawings

[00018] The solution will now be described in more detail by means of exemplary embodiments and with reference to the accompanying drawings, in which:

[00019] Fig. 1 is a block diagram illustrating the solution.

[00020] Fig 2 is a block diagram illustrating a power tool.

[00021] Fig. 3 is a flow chart illustrating a procedure in a power tool, according to possible embodiments.

[00022] Fig 4. is a signaling diagram illustrating an example of a delegation when the solution is used, according to further possible embodiments.

[00023] Fig. 5 is a communication scenario illustrating the solution, according to further possible embodiments.

[00024] Fig. 6 is a flow chart illustrating a procedure in a tool control node, according to possible embodiments.

[00025] Fig. 7A-C are illustrations of positioning scenarios for a power tool.

[00026] Fig. 8 illustrates examples of computer implementations.

[00027] Fig. 9 shows an illustration of relocation of a presence node.

Detailed description

[00028] Briefly described, a solution is provided to avoid theft of power tools and other capital intensive machineries related to construction sites. By having a lock on a power tool, which default is locked, it may be less attractive for theft. A lock which is remotely controlled. Only when a user is authorized by the owner of the tool, the tool is unlocked. The tool may be unlocked for a specific period of time. The tool may further be unlocked within a specific geographical or a specific volume. An unlock message may be transmitted from a tool control node, which instructs the power tool to be unlocked. The power tool is then unlocked and fully usable for a certain time period, before the time period has passed, a new unlock message must be received by the power tool, otherwise it will be locked for further usage. So if the tool does not receive any unlock message or, if the tool is outside a specified area, it will automatically be locked and unusable. An owner of a tool may for some reason want to revoke an authorization from a user to use the tool, for example if an invoice is not paid for. Then may the tool owner transmit a lock message to the tool, such it becomes unusable. The tool owner may delegate a right to transmit unlock and lock messages to an intermediate, a presence node. An example may be the tool rental company delegating to a site manager. Such right may also be revoked.

[00029] Now the solution will be described in more detail. Fig. 1 shows a block diagram with a power tool 100, a tool control node 110 for controlling power tools 100 and a presence node 120 for handling of delegated controlling of power tools 100.

[00030] Fig. 2 shows a block diagram of the tool 100. The tool includes a control unit 210 for controlling unlocking and locking of the power tool 100 and other actions. The power tool 100 further includes a counter 240 for counting of time. The power tool 100 further includes an actuator unit 250 for unlocking and locking of the power tool 100. The power tool may also include an energy supply unit 220,

a drive unit 230 and a communication unit 260 for reception and transmission of messages.

[00031] Power tool may also be denoted "device", appliances, powered machine, not limiting to other similar suitable terms. Appliances may include washer, dryer, dishwasher, heat pump, stove, oven, microwave, not limiting to other appliances used in a home or office. Tool control node may also be denoted "remote node" not limiting to other similar suitable terms. Presence node may also be denoted "mobile node" not limiting to other similar suitable terms. A few examples of the tool control node 110 may be, a server in a communications network, a virtual server in a communications network, a mobile phone or an application installed on a mobile phone, a PDA (Personal Digital assistant) or an application installed on a PDA, not limiting to other similar nodes. A few examples of a presence node 120 may be a mobile phone or an application installed on a mobile phone, a PDA (Personal Digital assistant) or an application installed on a PDA, a gateway, access switch, access router, WLAN access point (Wireless Local Area Network) not limiting to other similar nodes. The term "unlock" may also be denoted "enable", and the term "lock" may also be denoted "disabled".

[00032] Fig. 3 shows a method in a power tool 100 for enabling unlocking and locking of the power tool for prevention of unauthorized use. The method comprises receiving **S100** an unlock message to a control unit 210, the message including an instruction to unlock the tool 100. The method further comprises unlocking **S110** the power tool 100 according to the instruction by the control unit 210 via an actuator unit 250. The method further comprises counting **S120** an authorization time period from reception of the first message to the control unit 210 by a counter 230, wherein when the counted authorization time period exceed a predetermined threshold, the power tool 100 is locked **S130** by the control unit (210) via the actuator unit (250), thereby enabling prevention of unauthorized use of the power tool (100) by remote unlocking and locking.

[00033] The unlock message may come from a tool control node 110. The message may be carried via wireless radio communication, for example such as WiFi according to IEEE 802.11 (Institute of Electrical and Electronics Engineers), RFID (Radio-frequency identification), Bluetooth, not limiting to other similar communication methods. Protocols used for carrying the message may be Ethernet, TCP/UDP/IP (Transmission Control Protocol/User Datagram Protocol/Internet Protocol). Further examples of protocols which may be used are; SMTP (Simple Mail Transfer Protocol), SMS/MMS (Short Message Service / Multimedia Messaging Service), HTTP/HTTPS (Hypertext Transfer Protocol/Secure), SIP/SIPS (Session Initiation Protocol/Secure), not limiting to other suitable protocols for messages or communication with a power tool 100. The message with the unlock instruction may also include other information, such as a time stamp, or the length of the authorization time period, not limiting to other information. The authorization time period may be a time period during which the power tool 100 may be unlocked and prepared for normal operation. During the authorization time period, the power tool 100 may be outside radio contact with for example the tool control node 110. The counter 230 counts the authorization time period, such when the authorization time period exceeds the predetermined threshold the power tool 100 is locked. When the power tool 100 is locked it may not be possible to use for normal operation. The threshold may be adjusted, for example by manually setting a different value, or by reception of a different value via the unlock message or the lock message.

[00034] In an example of the solution, the actuator unit 250 may be at least one of electrical switch, mechanical lock and semiconductor based switch. Depending of the propulsion of the power tool 100 different kinds of locks may be more or less suitable. A combination of an electrical switch, mechanical lock and semiconductor based switch may be used for locking the power tool 100. In an example of the solution, when a second unlock message is received before the predetermined threshold is reached, the counter 230 may be restarted, such that the power tool 100 remains unlocked. By this action, the power tool 100 may be used in normal operation without interruption. Unless the counter 230 is restarted by for example

a second unlock message, the power tool 100 may be locked from normal operation. In an example of the solution, the unlock message may include a first key, wherein the first key may be required by the control unit 210 for authorization of the unlock message. By usage of the first key, it may be possible to authorize the unlock message or any other messages received by the tool 100. Thereby may the power tool 100 be enabled to protect itself from receiving or taking any actions based on unauthorized messages.

[00035] In an example of the solution, the drive unit 230 may require at least one of the first key or a second key from the control unit 110, for enabling of the drive unit 230. If the power tool for example has been stolen, and the control unit is replaced with a modified control unit, the power tool may then be prevented from unauthorized usage, because the drive unit may expect a correct key before propulsion of the power tool 100. In an example of the solution, a lock message may be received by the control unit 210, where the lock message may include an instruction to lock the tool 100, wherein the tool 100 may be locked by the control unit 210 via the actuator unit 250.

[00036] In an example of the solution, a position message including an alert signal is received by the control unit (210), the position message including an instruction to repeatedly transmit a response signal as a response to the alert signal, thereby enabling positioning of the tool (100). When a power tool 100 is missing, because it has been lost/misplaced or stolen, it may then be possible to position the tool. By the power tool 100 transmitting the response signal, it may then be possible to determine a distance to the power tool 100. It may also be possible to determine a direction to the power tool 100. It may also be possible to determine a position of the power tool 100. In an example of the solution showed in Fig. 4, the power tool 100 may be arranged to receive an alert signal from the control node 110. The alert signal may include an identification of the power tool 100, alerting the power tool 100 by matching the received identification with a preprogrammed identification of the power tool 100, transmitting a response signal to the alert signal, including the identification of the power tool 100 matching the

received identification, thereby enabling determination of the position of the power tool 100. In an example, the power tool 100 is adapted to repeatedly transmit the response to the alert signal. Hereby, a risk that for instance a control node 110 does not receive the response due to poor signal strength/connectivity resulting e.g. from the position of the power tool 100 or the presence node 120 may be reduced. Another advantage may be, if the power tool 100 changes locations, it may be possible to determine the new position.

[00037] Fig. 5, shows an overview of the solution from a positioning perspective, comprising a plurality of presence nodes 120. The solution may further comprise a tool control node 110 comprising for instance a presence node 120. The control node 110 is arranged to transmit a positioning request message, including an identification of the power tool 100, to a plurality of presence nodes 110. Such plurality of presence nodes may be a closed user group of users which have agreed to use a specific service, a random group of presence nodes 120 located in the vicinity of the control node 110, an open user community which users may subscribe to, an ad hoc network, or a meshed network, or similar. The control node 110 is further arranged to receive at least one response to the positioning request message, including a calculated distance to the power tool 100 from the presence node 120, and a position of the presence node 120 as well as determining a position of the power tool 100 by calculation of the distance of the power tool 100 from the presence node 120 in combination with the position of the at least one presence node 100. In an example of the solution, the control node 110 may be arranged to calculate the position of the power tool 100 using any of triangulation, multilateration or trilateration upon receiving responses to the position request message from a plurality of presence nodes 120. According to an embodiment, the control node 110 is hosted by a presence node 120, i.e. the control node 110 may itself be used to determine the position of the power tool 100.

[00038] In an example of the solution, the communication with the power tool 100 may be encrypted. By encryption of the communication between power tool 100

and other nodes, unauthorized access to the power tool 100 may be prevented, as well as man-in-the-middle types of attacks. In an example of the solution, the tool 100 may have a physical tamper protection. A physical tamper protection may prevent or reduce the risk of unauthorized physical access to the power tool 100. The physical tamper protection may also prevent or reduce the risk of unauthorized physical access to key components of the power tool 100.

[00039] Fig. 6 shows a flowchart of a method in a tool control node 110 for enabling unlocking and locking of a tool for prevention of unauthorized use. The method comprises transmitting an unlock message to the tool 100, where the message includes an instruction to unlock the tool 100. The method further includes counting an authorization time period from transmission of the unlock message to the tool 100, wherein when the counted authorization time period exceed a predetermined threshold, the method further comprises transmitting of a lock message including an instruction to lock the tool (100), thereby enabling prevention of unauthorized use of the tool 100 by remote unlocking and locking.

[00040] In an example of the solution, when a use time period end may be beyond the authorization time period end, a second unlock message may be transmitted to the tool 100 before the predetermined authorization time period threshold is reached, such that the power tool 100 remains unlocked. The authorization time period may for example be 24 hours, i.e. a power tool 100 may be used for up to 24 hours, and at the end of the 24 hours the power tool 100 may be locked from normal operation, unless a second unlock message may be transmitted from the tool control node 110 to the power tool 100. The authorization period may be in a range from seconds up to days or weeks, depending on practical implementation.

[00041] The use time period may be a time period of an intended use period on a construction site, for example a month. The use period may be in a range from single hours up to months or even years. A use time period may be possible to interrupt, or change to a shorter or longer period. An example is where a customer

of a rented power tool 100, may want to extend the rental period, or when a customer not has paid invoices, then the use time period may be extended, or interrupted. In the invoicing case, an unlock message may be transmitted from the tool control node 110 to the power tool 100, when the invoice is paid, such that the rental customer then may continue to use the power tool 100 under normal operation.

[00042] In an example of the solution, for example illustrated in Fig. 4, a position message including an alert signal may be transmitted to the power tool 100, thereby enabling positioning of the tool (100).

[00043] In an example of the solution, a delegated authorization to transmit unlock and lock messages to a specified power tool (100) message including the instruction to unlock the tool (100) may be transmitted to a presence node (120). Fig. 5 shows the tool control node 110, which may transmit the delegation to one of or all of the presence nodes 120:1, 120:B, 120:C. Fig. 5 also illustrated how the presence nodes 120:1, 120:B, 120:C may cooperate for positioning of a missing power tool 100. In an example of the solution, an annulation of the delegated authorization may be transmitted to the presence node (120).

[00044] The power tool 100, for example illustrated in Fig. 2, is adopted to enable unlocking and locking of the power tool 100 for prevention of unauthorized use. The power tool 100 is adopted to receive an unlock message to the control unit 210, where the message includes an instruction to unlock the tool 100. The power tool 100 is further adopted to unlock the power tool 100 according to the instruction by the control unit 210 via the actuator unit 250. The power tool 100 is further adopted to count an authorization time period from reception of the first message to the control unit 210 by the counter 230, wherein when the counted authorization time period exceed a predetermined threshold, the power tool 100 is locked by the control unit 210 via the actuator unit 250, thereby enabling prevention of unauthorized use of the power tool 100 by remote unlocking and locking.

[00045] Fig. 1 and Fig. 5 et. al. shows the tool control node 110 adopted to enable unlocking and locking of a tool for prevention of unauthorized use. The tool control node 110 is adopted to transmit the unlock message to the tool 100, the message including an instruction to unlock the tool 100. The tool control node 110 is further adopted count the authorization time period from transmission of the unlock message to the tool 100, wherein when the counted authorization time period exceed a predetermined threshold, tool control node 110 is adopted to transmit the lock message including an instruction to lock the tool 100, thereby enabling prevention of unauthorized use of the tool 100 by remote unlocking and locking.

[00046] Fig. 7A shows a block diagram over a situation wherein a power tool 100 is at a certain distance from a geographical point 840. The tool control node 110 may be arranged to determine whether the position of the power tool 100 is within a predefined distance D from the geographical point 840, or if the power tool 100 is outside the predetermined distance. According to one embodiment shown in 7B, the tool control node 110 determines the position by comparing the position of the power tool 100 with a set geographical point 840 and calculates the distance between them. According to another embodiment as is further disclosed in Fig. 7C, the geographical point 840 is defined by the location of a presence node 110. The position of the presence node 110 may be dynamic.

[00047] Now looking at Fig. 8. The power tool 100 and the tool control node 110 described above may be implemented, by means of program modules of a respective computer program comprising code means which, when run by processor "P" 250 causes the power tool 100 and the tool control node 110 to perform the above-described actions. The processor P 250 may comprise a single Central Processing Unit (CPU), or could comprise two or more processing units. For example, the processor P 250 may include general purpose microprocessors, instruction set processors and/or related chips sets and/or special purpose microprocessors such as Application Specific Integrated Circuits (ASICs). The processor P 250 may also comprise a storage for caching purposes.

[00048] Each computer program may be carried by computer program products "M" 260 in the power tool 100 and the tool control node 110, shown in Fig. 1, 2, 4, 5, et al, in the form of memories having a computer readable medium and being connected to the processor P. Each computer program product M 260 or memory thus comprises a computer readable medium on which the computer program is stored e.g. in the form of computer program modules "m". For example, the memories M 260 may be a flash memory, a Random-Access Memory (RAM), a Read-Only Memory (ROM) or an Electrically Erasable Programmable ROM (EEPROM), and the program modules m could in alternative embodiments be distributed on different computer program products in the form of memories within the power tool 100 and the tool control node 110.

[00049] In an example embodiment of the solution the technology could be used for authorization in relation to other purposes than theft prevention. Some power tools requires special skills from the operator and should therefore not be handled by any user, one example is a woodwork-class for educational purpose where some machines in the class room might be locked to a presence node 110 possessed by the teacher, hence preventing students from using machinery while the teacher is not in the vicinity. Another example is for use in DIY (do it yourself) tools for home users where the technology could be adapted as, for example, a child lock, allowing parents to store the power tools in areas were children potentially could locate them.

[00050] In the following a few examples of positioning techniques is described. The examples are for illustration of how a power tool 100 may be determined in direction, distance, and/or position. These examples are not limiting other techniques to be used.

[00051] Closest presence node 120. The most basic of the location determination techniques, is to identify the location based on the presence node 120 that is closest to the power tool 100. This may be done by looking at the association

between the power tool 100 and the presence node 120 or by measuring signal strength.

[00052] Calculation of the approximately distance between the power tool 100 and one or more presence nodes 120. This technique is called lateration. The distance may be calculated based on signal strength or timing information.

[00053] Received Signal Strength Indication (RSSI) - Signal strength is a measurement on how strongly a transmitted signal is being received at a particular distance from the transmitter. The signal strength varies with distance, obstacles and interfering radio frequency signals. Multi path fading also affect the signal strength. In Wi-Fi networks, the signal strength is defined as Received Signal Strength Indication (RSSI). RSSI may be measured by the presence node 120 Link Quality Indicator (LQI) is a metric of the current quality of the received signal. The LQI may provide an estimate of how easily a received signal may be demodulated by accumulating the magnitude of the error between ideal constellations and the received signal over the 64 symbols immediately following the sync word.

[00054] Time Difference of Arrival (TDoA, also time of flight) - Distance may be calculated based on signal propagation time. Radio waves travel at a known speed through the wireless medium. Thus, if the time of transmission and time of signal arrival are known, the distance may be computed. Time Difference of Arrival (TDoA) is an example of such a technique. In TDoA, the position may be computed based on the difference in time when the signal arrives at different presence nodes 120.

[00055] Angle (AoA) - Instead of timing information, angles may be used to calculate the position. At each access point, the wireless signal arrives at a certain angle. By using geometric relationships between the angles of arrival at two presence nodes 120, the estimated location may be computed.

[00056] Triangulation and Trilateration, - When the location is estimated based on angle measurements from three or more presence nodes 120 the method is referred to as triangulation. The signal strength or timing information from several access points may also be used together to form coverage circles and intersection points. If the distance from at least three different presence nodes 120 may be calculated, this technique is known as trilateration. With the use of algorithms, the power tool 100 most likely position may be pointed based on the information from the different presence nodes 120. The more presence nodes 120 that contribute in computing the location, the more likely it is to get an accurate approximation.

[00057] Location Patterning - None of the above position determination techniques take into account signal propagation characteristics, such as reflection, attenuation and multi-path fading. However, with the location patterning technique, such characteristics of the actual wireless medium considered in the position computation. This location patterning technique may need calibration, in order to record how the wireless signals propagate throughout the environment. During this calibration phase, RF characteristics and real world data regarding how obstacles affect the propagation may be collected and pre-stored in a database. This information may then be compared with real-time information from the presence nodes 120 to achieve a more accurate position approximation.

[00058] Multiple Range Estimation Locator MREL (Multiple Range Estimation Location) used with Andrews Location Measurement Units (LMUs). MREL may use the transmission time and the time of arrival of the signal to determine a circular range ring, where the power tool 100 may be located. The location may then estimated by the best intersection of the multiple range-rings. Conversely, TDoA calculates the difference in the time of arrival of the mobile signal between multiple pairs of receivers. The differences in arrival time determine hyperbolic curves between receivers of where the power tool 100 may be. The location may then be estimated by the best intersection of the multiple hyperbolic curves.

[00059] In an embodiment, distance or position may be determined by usage of at least one of: association or signal strength, timing information, Received Signal Strength Indication (RSSI), Link Quality Indicator (LQI), Time Difference of Arrival/Time-of-Arrival (TDoA/TOA), Angle (AoA), Triangulation and/or Trilateration, Location Patterning, Multiple Range Estimation Locator MREL (Multiple Range Estimation Location), in combination with anyone else of the mentioned solutions.

[00060] Fig. 9 illustrates an embodiment of the solution. A presence node 120 may be relocated to different positions. The different positions may be represented in a coordinate system. An example is where the start point of the presence node 120 is determined as coordinate "0". When the presence node 120 is relocated and at each point where a signal is received from the power tool 100, the new coordinate is determined. There by it may be possible to by usage of one presence node 120 simulate a plurality of presence nodes 120, where the simulated plurality of presence nodes 120 may better determine a position of a power tool 100, than a single presence node 120. A presence node 120 may determine its coordinate by use of GPS, etc. The presence node 120 may also determine a relative coordinate by usage of for example one of gyro, magnetic compass, accelerometer, tilt sensor, gyroscope, altimeter, not limiting to other type of sensors for measuring movements and/or relative positions.

[00061] In an embodiment, not shown in Fig. 9, the coordinate system may be a three dimensional coordinate system, such when a presence node 120 is relocated and during the relocation determines three dimensional coordinates for each signal received from the power tool 100.

[00062] A user of a presence node 120 may by moving around, simulate a group of users where each user has a presence node 120, thereby it may be possible to better determine a position of a power tool 100 than with a single presence node 120 stationary at one point.

[00063] In an embodiment, the time difference of arrival is measured by the power tool 100, instead of the presence node 120. An illustrative example is where at least one presence node 120 transmits a signal, such an alert signal or any other signal, such that the power tool 100 may measure the time of flight from the presence node 120 to the power tool 100. The power tool 100 may transmit the response to the alert signal, or any other signal, the response including the identification of the power tool 100 and also the measured transmission time between the presence node 120 and the power tool 100. The power tool 100 may additionally, based on the measured transmission time between the presence node 120 and the power tool 100, determine the distance between the presence node 120 and the power tool 100. The response transmitted by the power tool 100 may then include: identification of the power tool 100, measured transmission time between the presence node 120 and the power tool 100, and the determined distance between the presence node 120 and the power tool 100. In an embodiment, the time may be measured with an accuracy down to microseconds. In another embodiment, the time may be measured with an accuracy down to nanoseconds.

[00064] There may be advantages with the power tool 100 measuring the time of arrival, time difference of arrival or time of flight, instead of the presence node 120. An advantage may be that the power tool 100 may be easier to adopt for measuring the signals time of flight, than adopting the presence node 120 for measuring the time. Another advantage may be that the power tool 100 may be adapted to measure time with a better accuracy. Another advantage may be that by performing measurement in the device, more presence nodes 120 may participate in positioning a power tool 100 with a better accuracy than only presence node 120 with support for measuring the time. Another advantage with measuring time in the power tool 100 is that a plurality of additional sources for determination of the distance between a mobile terminal and a power tool 100 may enable avoidance of signal reflections and other disturbances.

[00065] In a situation where there is a plurality of presence nodes 120, the power tool 100 may transmit a response to each presence node 120, from which the power tool 100 has received a valid identification. The response may include any of: the identification, measured transmission time, and determined distance. The plurality of presence nodes 120 may better determine the position of the power tool 100.

[00066] The presence nodes can further be utilized for positioning of tools through Time of Arrival. Such positioning is not limited to peer-to-peer networks and can thereby be any form of network communication, comprising other network communication units such as for example access points.

[00067] According to one aspect of the present solution, a method is provided wherein a first node for determining the distance between two nodes in a communication network utilizes the media access control layer (MAC-layer) present in multiple standards, such as the IEEE 802.11x standard.

[00068] It has been shown that network communication conducted within the MAC-layer without the involvement of higher level layers provide processing times that are relatively constant. The MAC-layer is adapted to communicate the information of high level layers as one of its tasks but some frames can be transmitted standalone by the MAC-layer. By utilizing those frames, and/or, modifying behavior of a MAC-layer in a wireless communication network by adding additional features, processing times can be changed from an unreliable and changeable time factor to an approximated constant. The possibility to approximate the processing time makes it possible to subtract the processing time and utilize Time of Arrival / Time of Flight measurements. The methods described below thereby provide an enhanced system for determining the distance between two nodes in a communication network by significantly reduce the problem of previous methods.

[00069] This can be done in an open user community, as previously described, wherein users subscribes to, an ad hoc network, or a meshed network, or similar.

Such method can for example be conducted in a first presence node adapted for determining the distance between said first presence node and a second presence node in a wireless communication network. The first presence node comprises a network communication unit with a medium access control layer (MAC-Layer), and the first presence node performs a method comprising the steps:

- transmitting a response request message,
- starting a first counter at transmission of said response request message,
- receiving a response to said response request message,
- stopping the counter at reception of the response to said response request message,
- determining based on the counter result the distance between said first and second presence node,

wherein

said counter result is the period from transmission of said response request message to the arrival of said response in the medium access control layer (MAC-Layer) of said first presence node network communication unit.

[00070] Positioning could also be accomplished through nodes in a wireless communication network, comprising a network communication unit with a medium access control layer (MAC-Layer), said node configured to calculate the Time of Arrival and/or Time of Flight based on a counted time from transmission of a response request message in the medium access control layer of said node to the corresponding arrival of a response to said response request message in the medium access control layer (MAC-Layer) of said node.

[00071] The counter can in one embodiment count processor cycles based on for example a central processing unit clock frequency. It is further understood that the counter can be any means arranged in a node, or attached hardware or software, which can directly or indirectly be used to determine a passed time.

[00072] For enablement of positioning determination through Time of Arrival based on MAC-Layer communication, an additional clock may be added to at least

one node in a wireless communication network that uses a higher clock frequency than the standard clock. For example, in an IEEE 802.11x wireless communication network system the 1 MHz clock frequency may be complemented with an additional clock that provides better resolution for distance determination. In a preferred embodiment is such a complementary clock arranged with a frequency at 30-50 MHz, 50-500 MHz, 100 MHz or higher, or approximately 40 MHz.

[00073] RTS and CTS messages are handled in the MAC-layer of a network communication unit structure and thereby have the advantage of relatively stable processing times. This applies not only between different version of the same node but also between different sorts of nodes, such as mobile phones, access points, Wi-Fi-tags, etc. Furthermore, RTS and CTS messages are part of some wireless network communication standards and are thereby always present in devices following those standards.

[00074] For the determination of the position, wireless communication networks, such as for IEEE 802.11x, Bluetooth, ZigBee, or any other wireless communication network can be used. For example, a first presence node transmits a Request-to-Send message (RTS) and a second presence node response with a Clear-to-Send message (CTS) before any data is transferred. The RTS and CTS messages may be handled in the MAC-Layers of both the first presence node and the second presence node and may be thereby not affected of processing times in the CPUs of the nodes. The Time of Arrival / Time of Flight can thereby be calculated and used for distance determination and positioning.

[00075] It is further understood that different frequencies could be used. For example could frequencies from 400 MHz up to 5,5 GHz preferably be used in different embodiments of the invention.

[00076] While the solution has been described with reference to specific exemplary embodiments, the description is generally only intended to illustrate the inventive concept and should not be taken as limiting the scope of the solution. For example, the terms "power tool", "appliances", "presence node" and "tool control

node" have been used throughout this description, although any other corresponding nodes, functions, and/or parameters could also be used having the features and characteristics described here. The solution is defined by the appended claims.

The Swedish Patent Office
PCT International Application
1

PCT/SE2013/051595
27-01-2015

CLAIMS

1. A method in a power tool (100) for enabling unlocking and locking of a power tool for prevention of unauthorized use, the method comprising:
 - receiving (S100) a message to a control unit (210), the message including an instruction to unlock the power tool (100),
 - unlocking (S110) the power tool (100) according to the instruction by the control unit (210) via the actuator unit (250), thereby enabling prevention of unauthorized use of the power tool (100) by remote unlocking,
 - counting (S120) an authorization time period from reception of the first unlock message to the control unit (210) by a counter (230),
 - when a second unlock message is received before a predetermined threshold of the authorization time period is reached the counter (230) is restarted, such that the power tool (100) remains unlocked,
 - a position message including an alert signal is received by the control unit (210), the position message including an instruction to repeatedly transmit a response signal as a response to the alert signal, thereby enabling positioning of the tool (100), and
 - when the predetermined threshold of the counted authorization time period is reached, locking (S130) the power tool (100) according to the instruction by the control unit (210) via an actuator unit (250).
2. The method according to claim 1, wherein:
 - the actuator unit (250) is at least one of electrical switch, mechanical lock and semiconductor based switch.

AMENDED SHEET

3. The method according to any of claims 1-2, wherein:

- the unlock message includes a first key, wherein,
- the first key is required by the control unit (210) for authorization of the message.

4. The method according to any of claims 1-3, wherein:

- the drive unit (230) require at least one of the first key or a second key from the control unit (110), for enabling of the drive unit (230).

5. The method according to any of claims 1-4, wherein:

- a lock message is received by the control unit (210), the lock message including an instruction to lock the tool (100), wherein
- the tool (100) is locked by the control unit (210) via the actuator unit (250).

6. The method according to any of claims 1-5, wherein:

- a message including an alert signal is received by the control unit (210);
- said message triggers the control unit (210) to transmit a signal requesting response signals from presence nodes nearby;
- receiving response signals to the control unit (210) from presence nodes (120:A, 120:B, 120:C) nearby and thereby enabling positioning of the tool (100).

7. The method according to any of claims 1-6, wherein:

- the communication with the tool (100) is encrypted.

8. A method in a tool control node (110) for enabling unlocking and locking of a tool for prevention of unauthorized use, the method comprising:

- transmitting an unlock message to the tool (100), the message including an instruction to unlock the tool (100),
- counting an authorization time period from transmission of the unlock message to the tool (100),
- when a use time period end is beyond the authorization time period end, transmitting a second unlock message to the tool (100) before the predetermined authorization time period threshold is reached, such that the power tool (100) remains unlocked,
- transmission of a position message including an alert signal to the power tool (100), thereby enabling positioning of the tool (100),
- when the counted authorization time period exceed a predetermined threshold,
- transmitting a lock message including an instruction to lock the tool (100), thereby enabling prevention of unauthorized use of the tool (100) by remote unlocking and locking.

9. The method according to claim 8, wherein:

- transmitting a delegated authorization to transmit unlock and lock messages to a specified power tool (100) message including the instruction to unlock the tool (100) to a presence node (120).

10. The method according to any of claims 8-9, wherein:

PCT/SE2013/051595
27-01-2015

4

- transmitting an annulation of the delegated authorization to the presence node (120).

11. A method in a presence node (120) for enabling unlocking and locking of a tool for prevention of unauthorized use, the method comprising:

- transmitting an unlock message to the tool (100), the message including an instruction to unlock the tool (100),
- counting an authorization time period from transmission of the unlock message to the tool (100),
- when a use time period end is beyond the authorization time period end,
- transmission of a second unlock message to the tool (100) before the predetermined authorization time period threshold is reached, such that the power tool (100) remains unlocked,
- transmission of a position message including an alert signal to the power tool (100), thereby enabling positioning of the tool (100),
- when the counted authorization time period exceed a predetermined threshold, and
- transmitting of a lock message including an instruction to lock the tool (100), thereby enabling prevention of unauthorized use of the tool (100) by remote unlocking and locking.

12. A power tool (100) arranged to enable unlocking and locking of said power tool (100) for prevention of unauthorized use, the power tool (100) further arranged to:

- receive a message to a control unit (210), the message including an instruction to unlock or lock the tool (100),
- lock or unlocking the power tool (100) according to the instruction by the control unit (210) via the actuator unit (250), thereby enabling prevention of unauthorized use of the power tool (100) by remote unlocking and locking,
- wherein, the control unit (210) is arranged to receive a position message including an alert signal, the position message including an instruction to repeatedly transmit an response signal as a response to the alert signal, thereby enabling positioning of the tool (100).

13. The power tool (100) according to claim 12, adopted to:

- count an authorization time period from reception of the first message to the control unit (210) by a counter (230), wherein when the counted authorization time period exceed a predetermined threshold,
- lock the power tool (100) according to the instruction by the control unit (210) via an actuator unit (250).

14. The power tool (100) according to claim 12 or 13, wherein:

- the actuator unit (250) is at least one of electrical switch, mechanical lock and semiconductor based switch.

15. The power tool (100) according to claims 12-14, adopted to:

- when a second unlock message is received before the predetermined threshold is reached,
- restart the counter (230), such that the power tool (100) remains unlocked.

16. The power tool (100) according to any of claims 12-15, wherein:

- the unlock message includes a first key, wherein,
- the first key is required by the control unit (210) for authorization of the message.

17. The power tool (100) according to any of claims 12-16, wherein:

- the drive unit (230) is arranged to require at least one of the first key or a second key from the control unit (110), for enabling of the drive unit (230).

18. The power tool (100) according to any of claims 12-17, wherein:

- the control unit (210) is arranged to receive a lock message including an instruction to lock the tool (100), wherein
- the actuator unit (250) is arranged to be locked by the control unit (210) via the actuator unit (250).

19. The power tool (100) according to any of claims 12-18, wherein:

- the control unit (210) is arranged to receive a message including an alert signal;
- said message triggers the control unit (210) to transmit a signal requesting

response signals from presence nodes nearby;

- the control unit (210) is arranged to receive response signals from presence nodes (120:A, 120:B, 120:C) nearby and thereby enabling positioning of the tool (100).

20. The power tool (100) according to any of claims 12-19, arranged to:

- use encrypted communication.

21. The power tool (100) according to any of claims 12-20, wherein:

- the tool (100) has a physical tamper protection.

22. A tool control node (110) adopted to enable unlocking and locking of a tool for prevention of unauthorized use, the node adopted to:

- transmit an unlock message to the tool (100), the message including an instruction to unlock the tool (100),

- count an authorization time period from transmission of the unlock message to the tool (100), wherein when the counted authorization time period exceed a predetermined threshold,

- transmit of a lock message including an instruction to lock the tool (100), thereby enabling prevention of unauthorized use of the tool (100) by remote unlocking and locking, and

- the power tool control node (110) is adopted to perform the method according to any claims 8-10.

23. A computer program, comprising computer readable code means, which when run in a power tool (100) is arranged to enable unlocking and locking of the power tool (100) according to any of the claims 12 to 21 and causes the power tool (100) to perform the corresponding method according to any of the claims 1 to 7.

24. A computer program, comprising computer readable code means, which when run in a tool control node (110) is arranged to enable unlocking and locking of power tool (100) according to any of the claims 12 to 21 and causes the tool control node (110) to perform the corresponding method according to any of the claims 8 to 10.

25. A computer program, comprising computer readable code means, which when run in a presence node (120) is arranged to enable unlocking and locking of a power tool (100) according to any of the claims 12 to 21 and causes the presence node (120) to perform the corresponding method according to any of the claims 8 to 10.

26. A computer program product, comprising a computer readable medium and a computer program according to any of claim 23-25, wherein the computer program is stored on the computer readable medium.

1/9

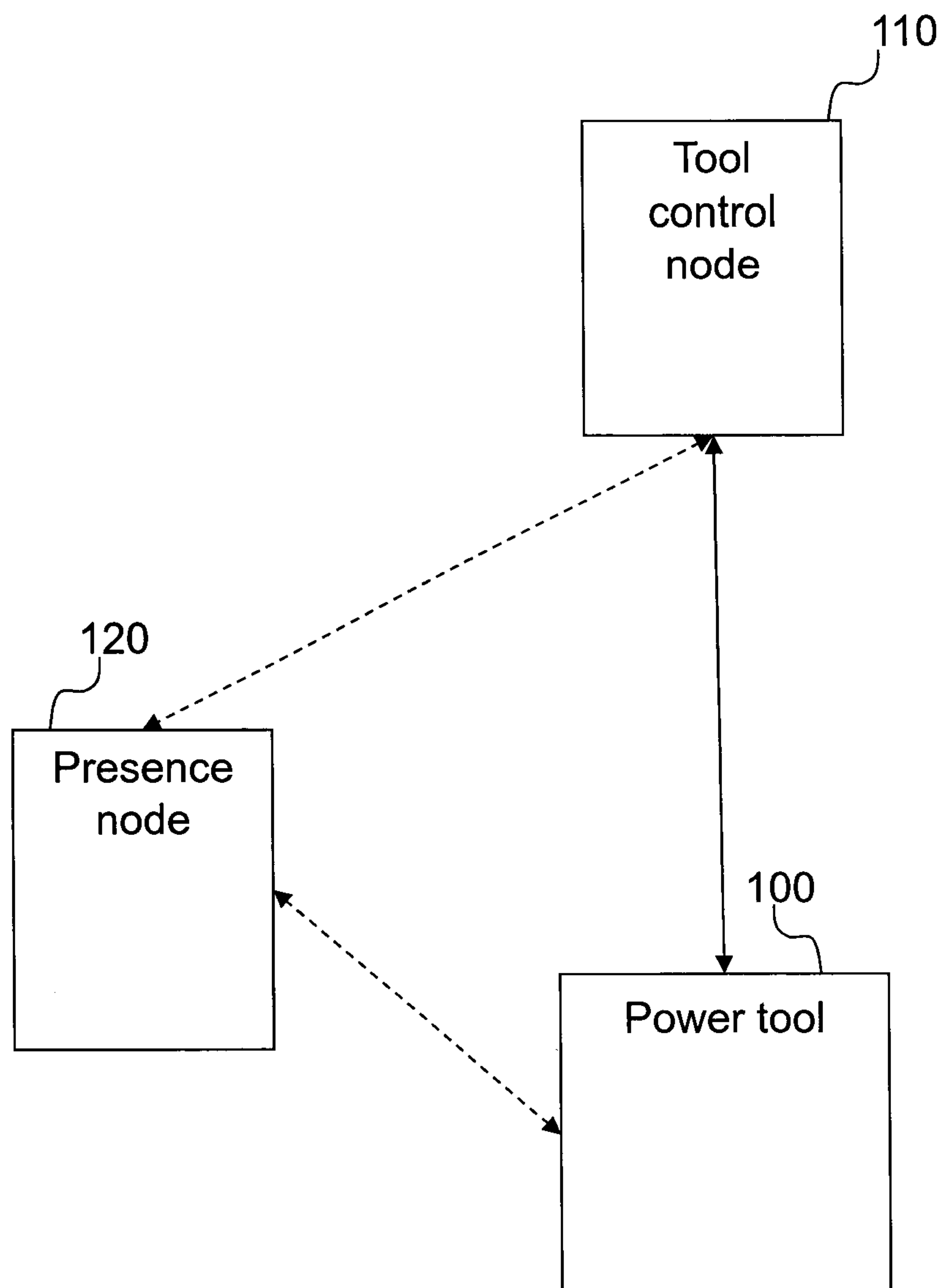


Fig. 1

2/9

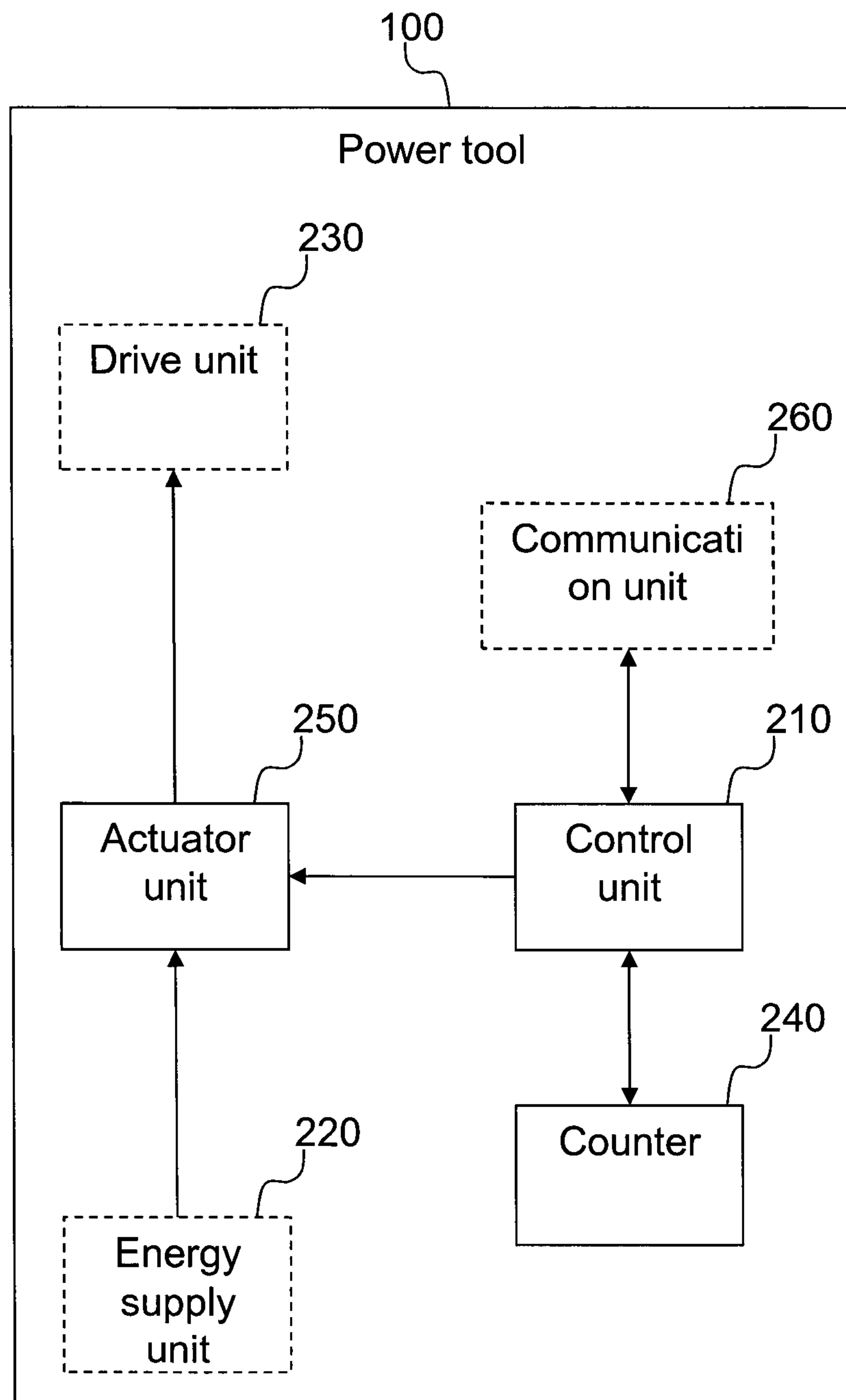


Fig. 2

3/9

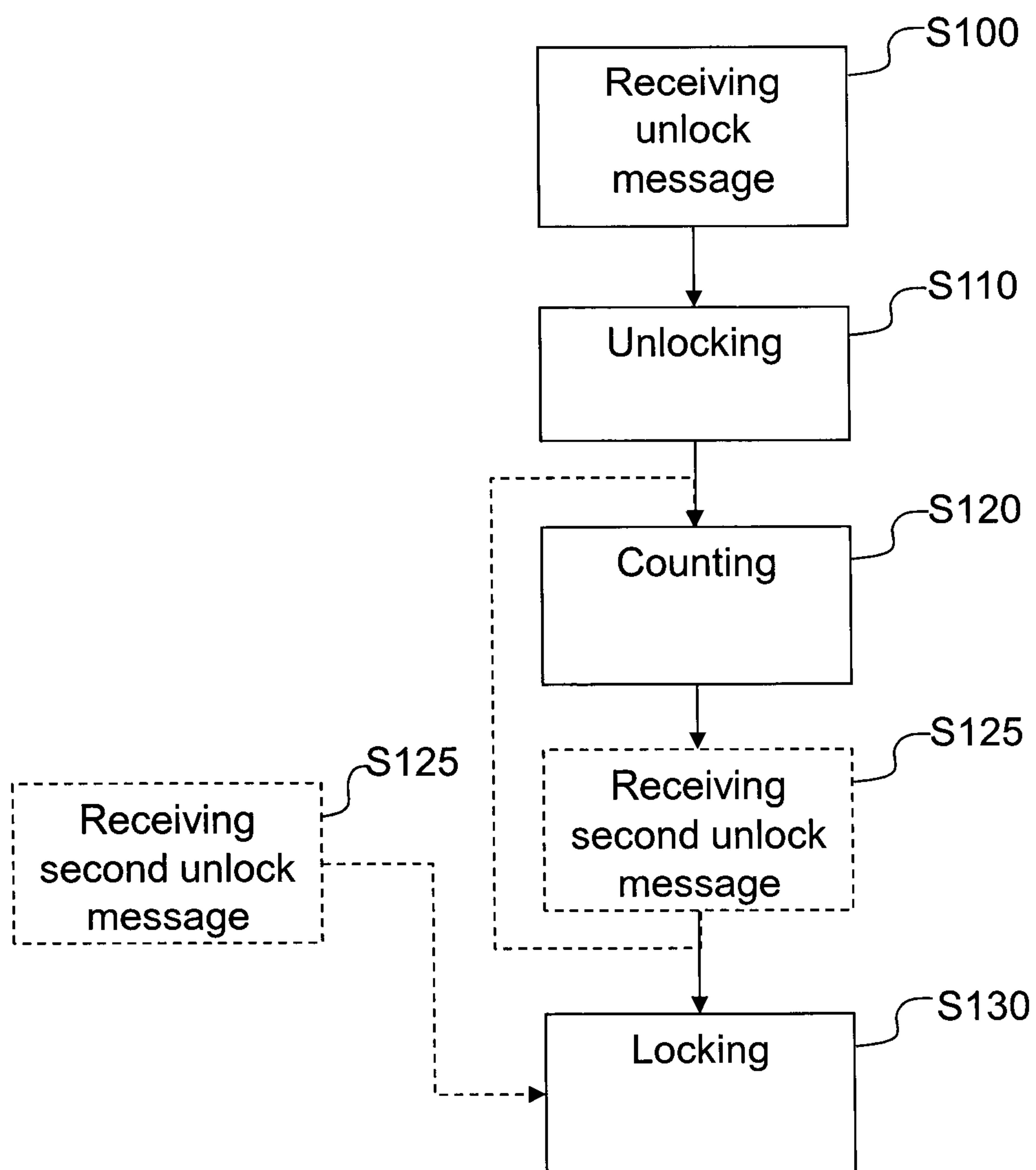


Fig. 3

4/9

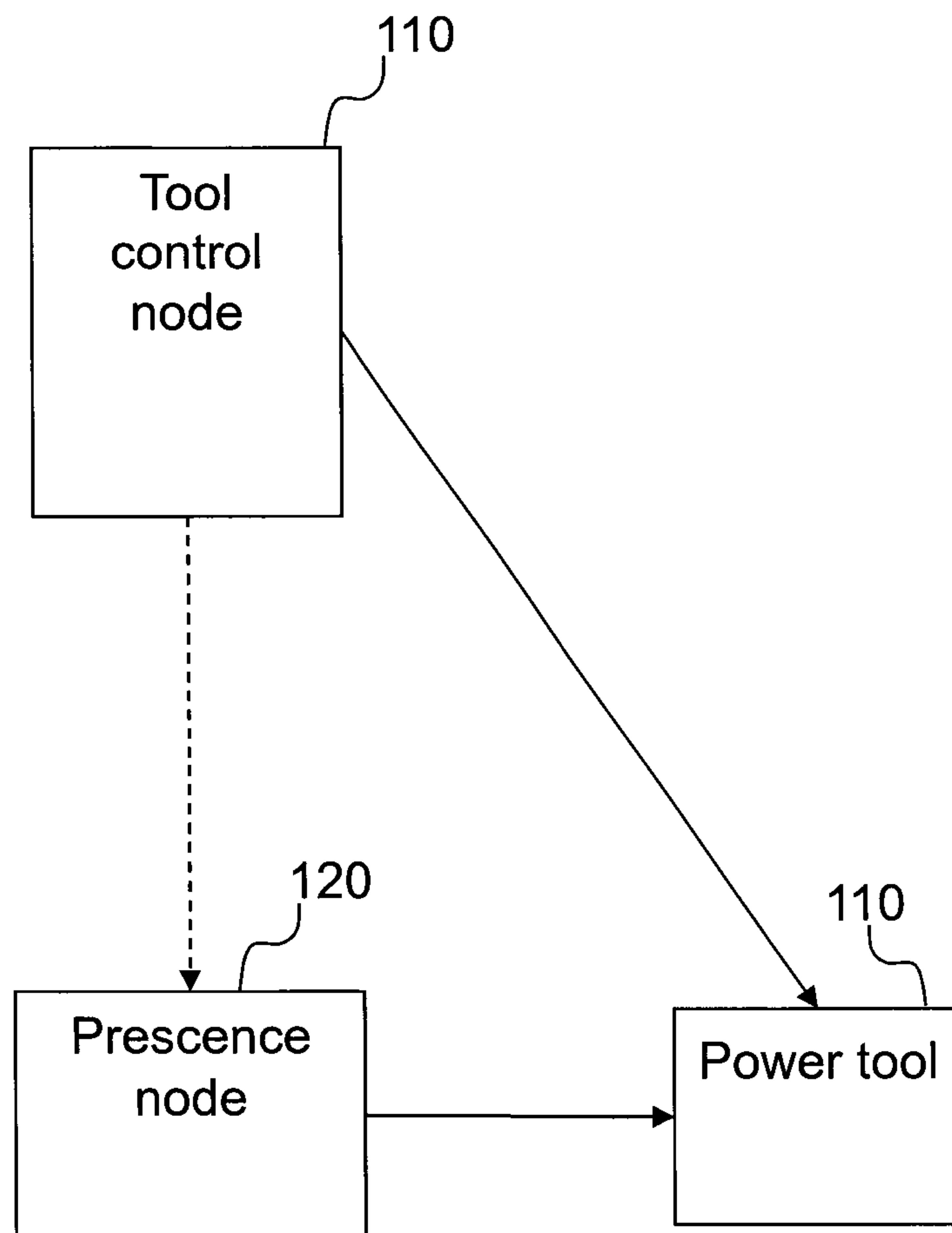


Fig. 4

5/9

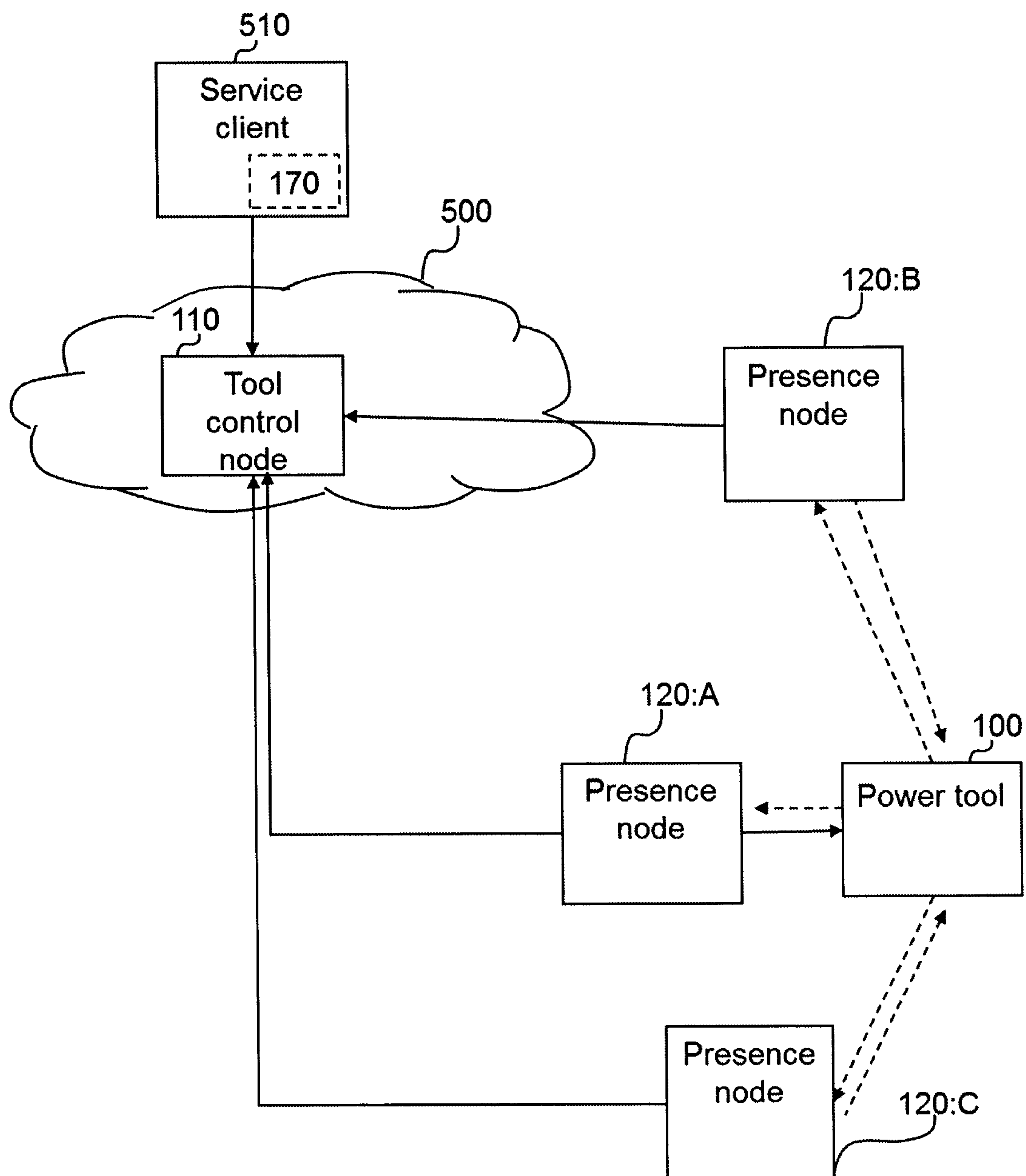


Fig. 5

6/9

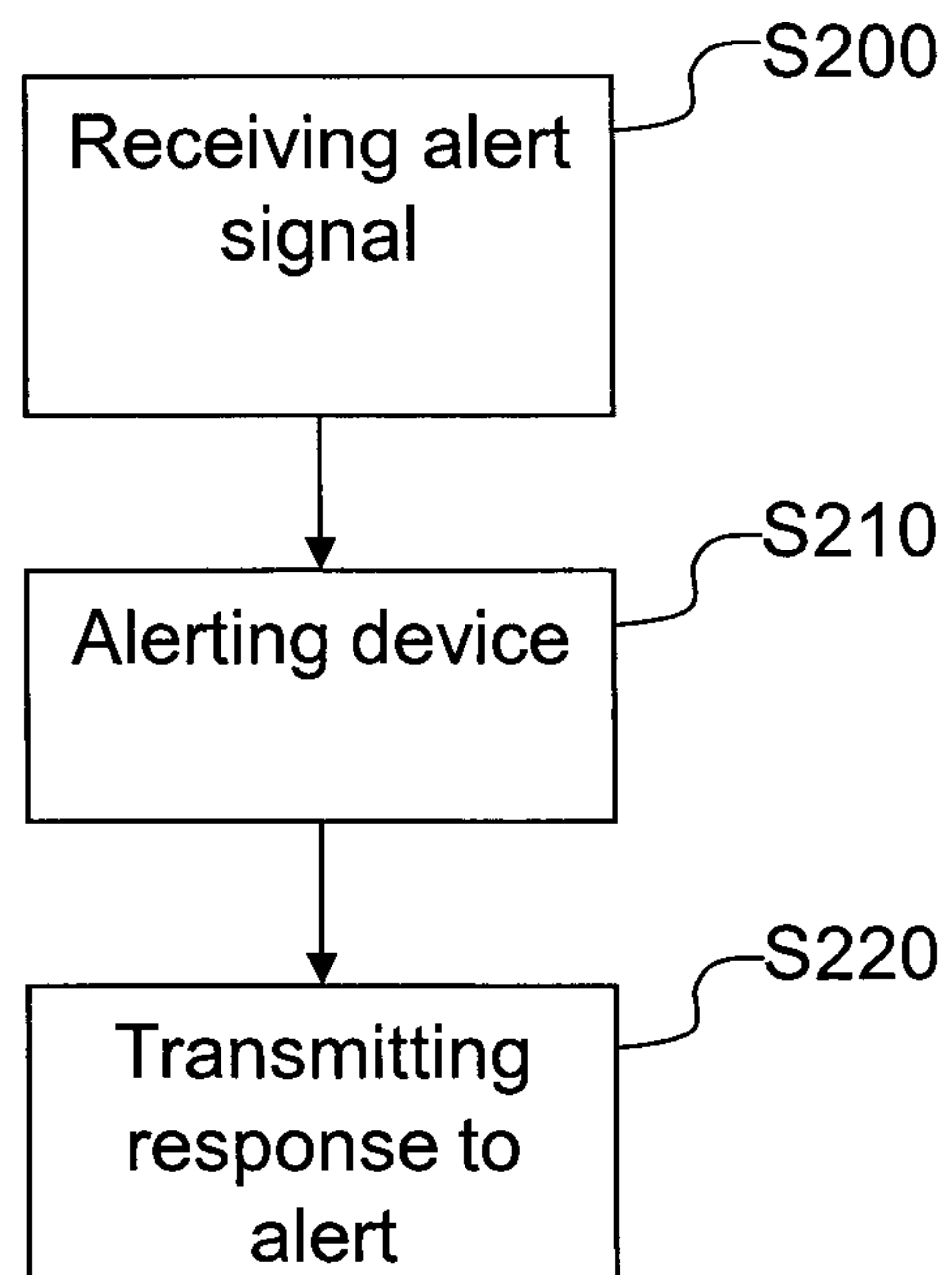


Fig. 6

7/9

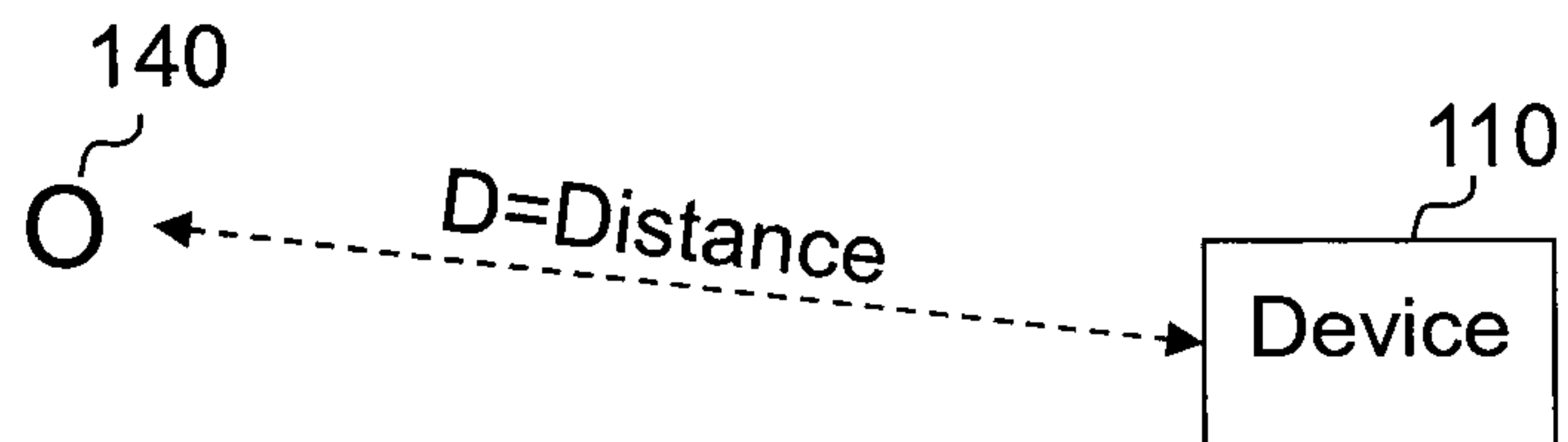


Fig. 7A

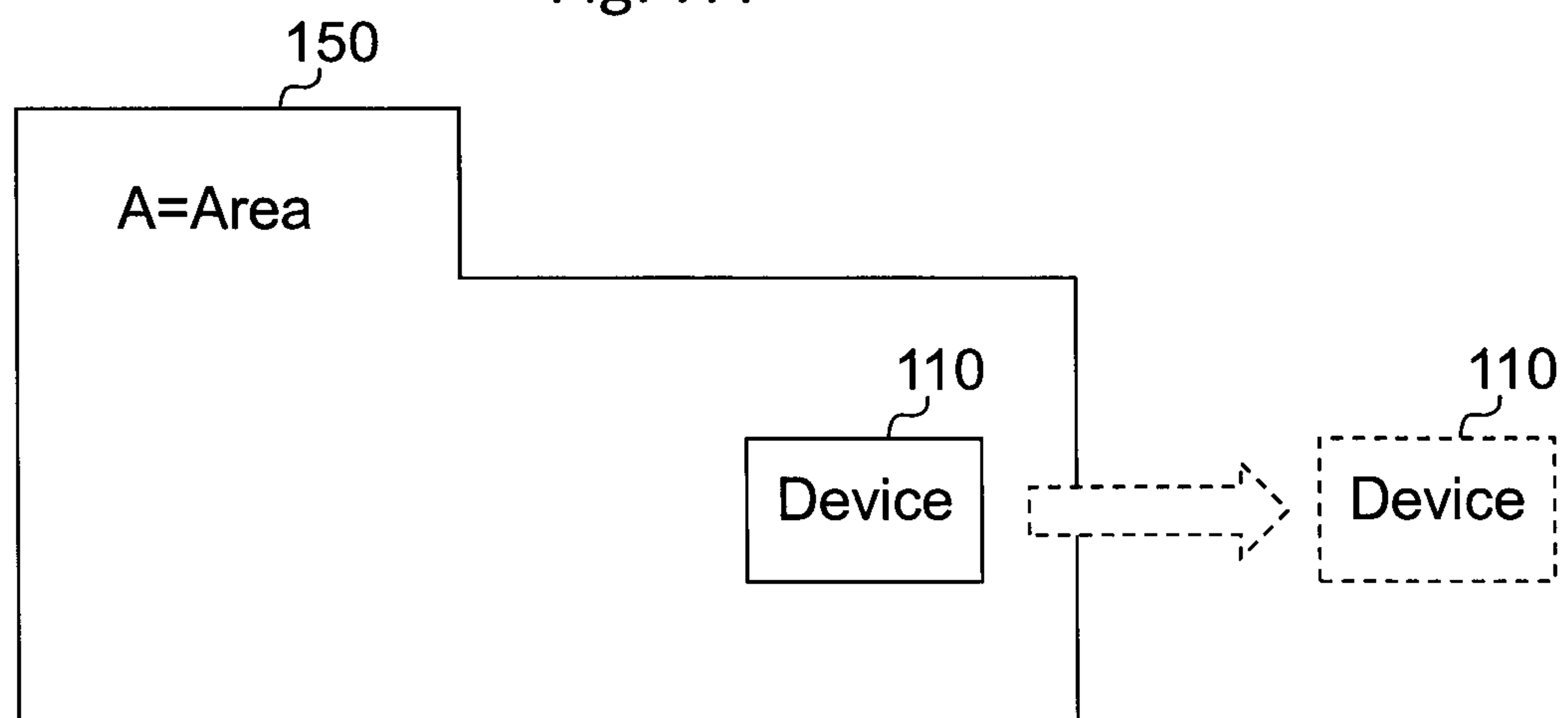


Fig. 7B

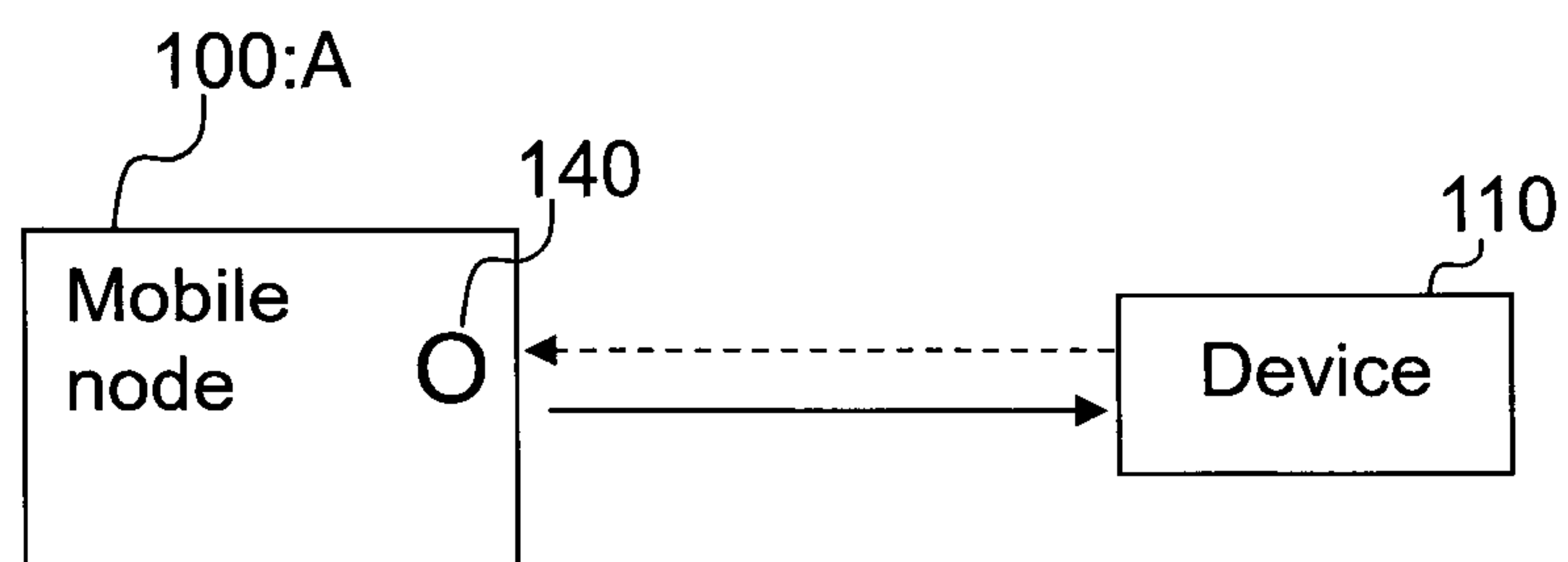


Fig. 7C

8/9

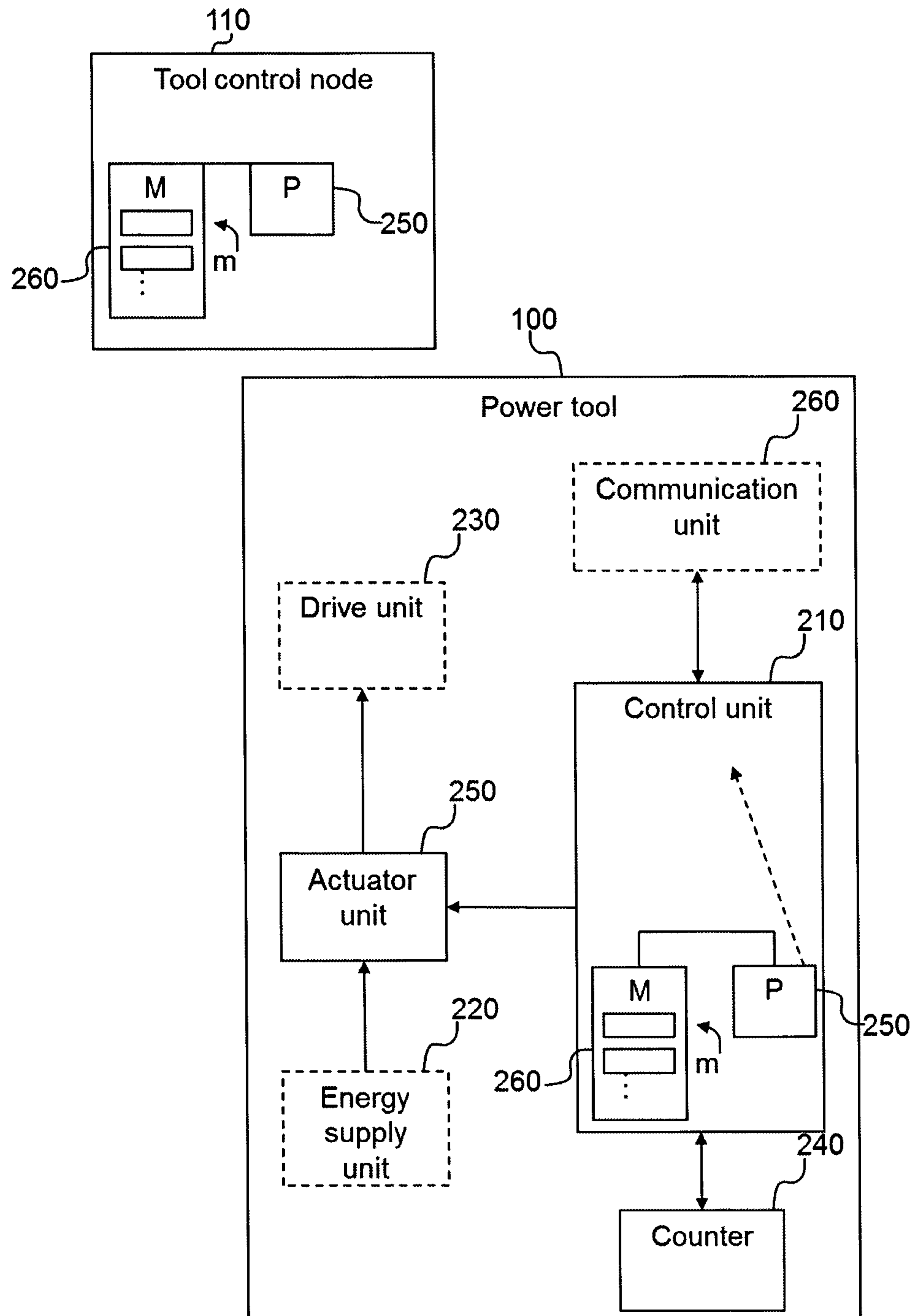


Fig. 8

9/9

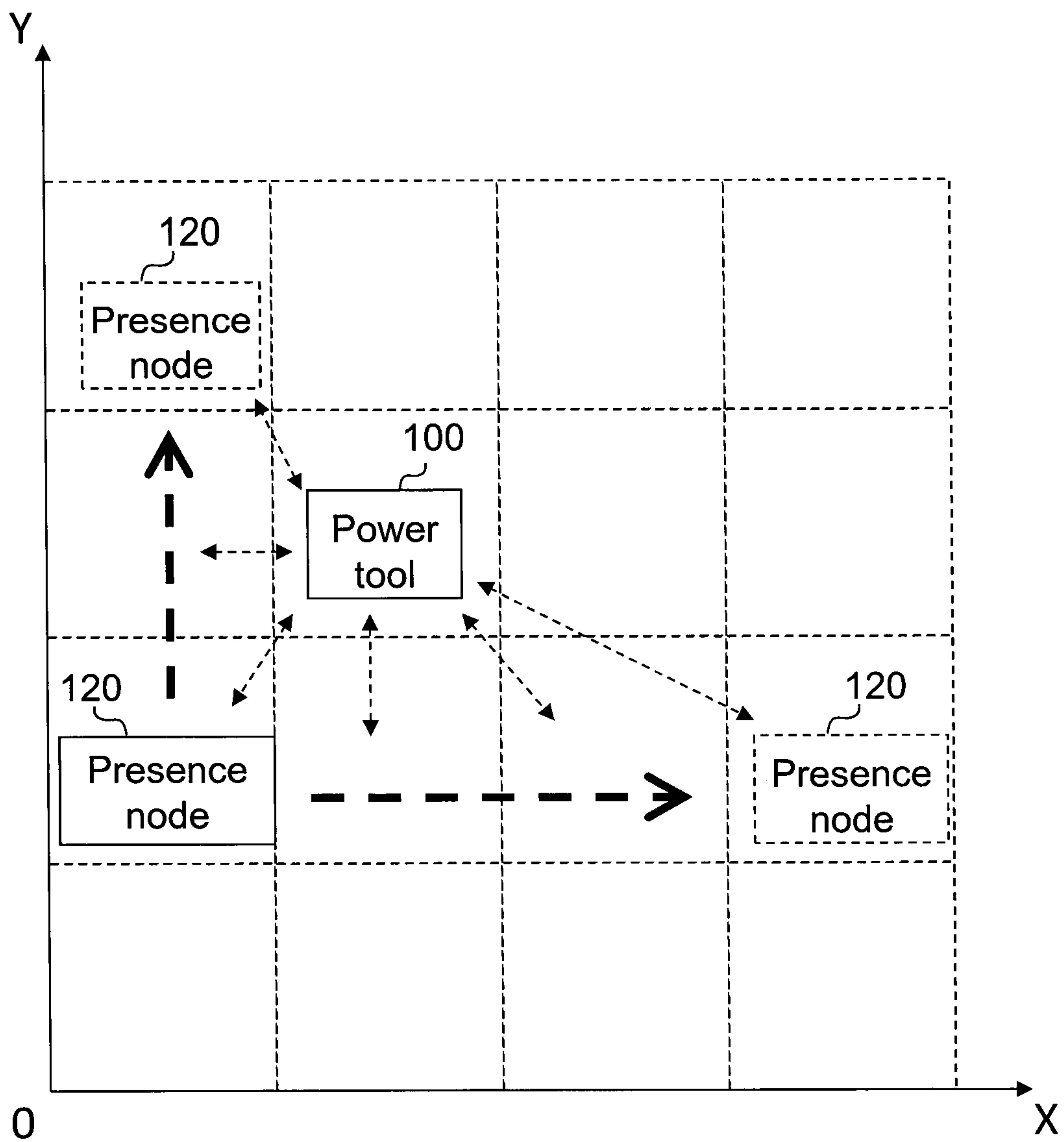


Fig. 9

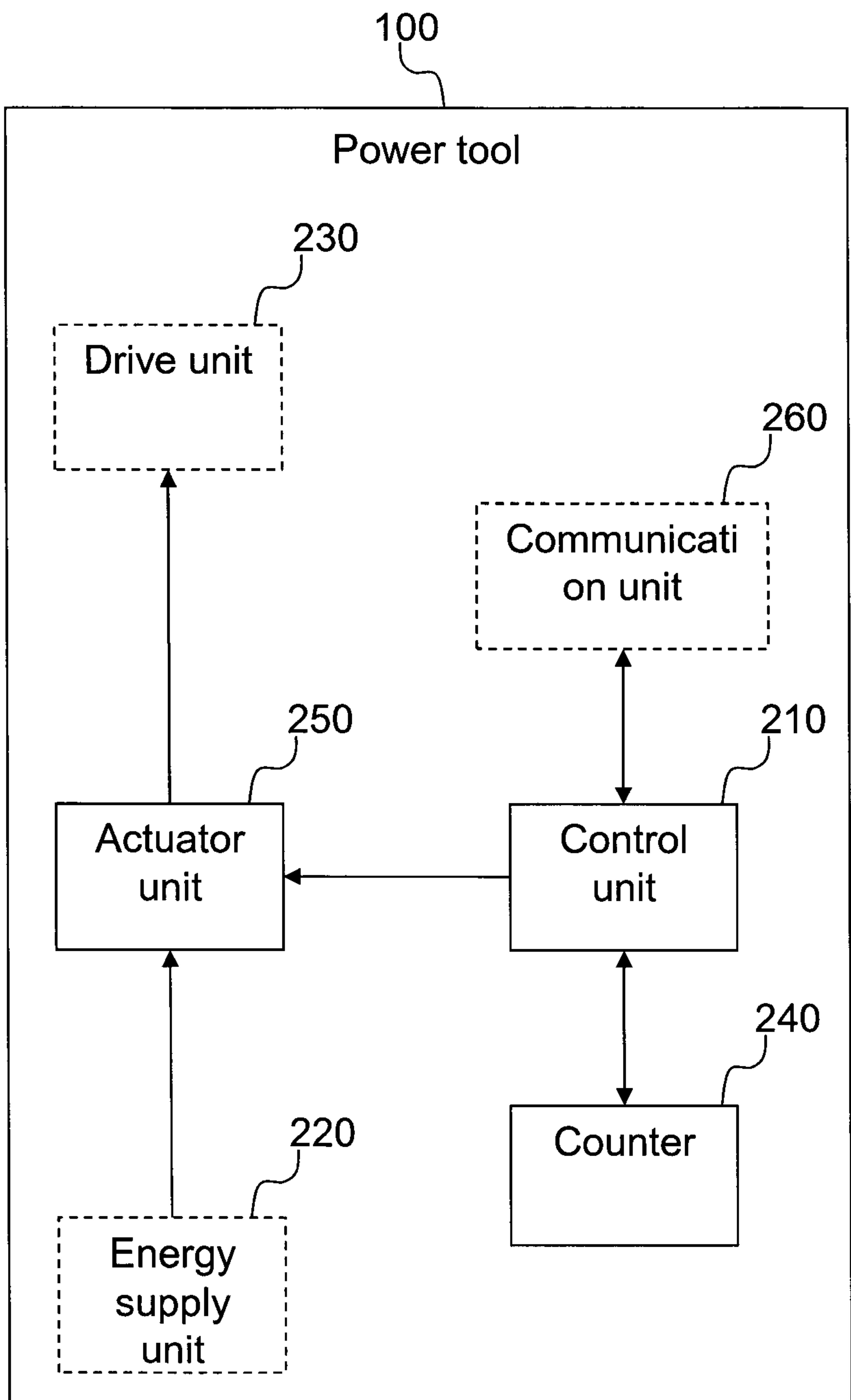


Fig. 2