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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 June 2019 (13.06.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/109210 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2017/114458

(22) International Filing Date:
04 December 2017 (04.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and
(71) Applicant *(for SC only)*: **HUANG, Yang** [CN/CN]; No.5 Lize East Street, Chaoyang District, Beijing 100102 (CN).

(72) Inventors: **CHEN, Shi**; No.5 Lize East Street, Chaoyang District, Beijing 100102 (CN). **LIU, Wenzhao**; No.5 Lize East Street, Chaoyang District, Beijing 100102 (CN).

(74) Agent: **ZHONGZI LAW OFFICE**; 7F, New Era Building, 26 Pinganli Xidajie, Xicheng District, Beijing 100034 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

WO 2019/109210 A1

(54) Title: NETWORK MANAGEMENT DEVICE AND CENTRALIZED AUTHORIZATION SERVER FOR NETCONF

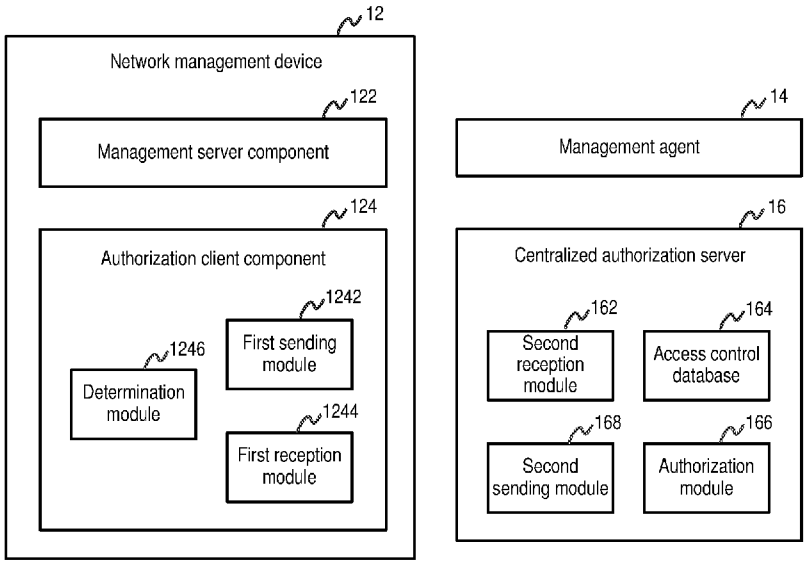

FIG. 1

(57) Abstract: A network management device and a centralized authorization server are disclosed for network configuration (NETCONF) protocol. The network management device comprises a management server component and an authorization client component. The management server component is configured, with NETCONF protocol, to process a user operation request from a management agent based at least on authorization information from the authorization client component. The authorization client component is configured, with a remote authorization protocol, to obtain, for the user operation request, the authorization information from the centralized authorization server.

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

NETWORK MANAGEMENT DEVICE AND CENTRALIZED AUTHORIZATION SERVER FOR NETCONF

Technical Field

[0001] Embodiments of the disclosure generally relate to network communication, and, more particularly, to a network management device and a centralized authorization server for network configuration (NETCONF) protocol.

Background

[0002] This section introduces aspects that may facilitate better understanding of the present disclosure. Accordingly, the statements of this section are to be read in this light and are not to be understood as admissions about what is in the prior art or what is not in the prior art.

[0003] With the development of cloud computing technologies, software defined network (SDN) has been proposed to facilitate network management and enable programmatically efficient network configuration. In the evolving could/SDN infrastructure, the dominant northbound interface is network configuration (NETCONF) protocol, which is a network management protocol developed and standardized by the Internet engineering task force (IETF). The first version of the base NETCONF protocol was published as request for comments (RFC) 4741 in December 2006. Several extensions were published in subsequent years. One of the extensions is RFC 6536 published in March 2012. It proposed an authorization solution, called NETCONF access control model (NACM), to restrict NETCONF protocol access for particular users to a pre-configured subset of all available NETCONF protocol operations and content.

[0004] For the above existing authorization solution, there is still some room for improvement.

Summary

[0005] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the detailed description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

[0006] One of the objects of the disclosure is to provide an improved authorization solution for NETCONF protocol.

[0007] According to one aspect of the disclosure, there is provided a network management device. The network management device comprises a management server component and an authorization client component. The management server component is configured, with NETCONF protocol, to process a user operation request from a management agent based at least on authorization information from the authorization client component. The authorization client component is configured, with a remote authorization protocol, to obtain, for the user operation request, the authorization information from a centralized authorization server.

[0008] In an embodiment of the disclosure, the remote authorization protocol is terminal access controller access-control system plus (TACACS+) protocol or remote authentication dial in user service (RADIUS) protocol.

[0009] In an embodiment of the disclosure, the management server component is configured to convert the user operation request to an operation identification and an Xpath. The Xpath represents an object on which the operation is to be performed. The authorization client component comprises a first sending module, a first reception module and a determination module. The first sending module is configured to send to the centralized authorization server an authorization request including the operation identification and the Xpath. The first reception module is configured to receive an authorization response from the centralized authorization server. The determination module is configured to determine the authorization information based on the authorization response.

[0010] In an embodiment of the disclosure, there are multiple operations indicated in the user operation request. The first sending module and the first reception module operate iteratively for each of the multiple operations. The determination module is configured to determine the authorization information as failure when the authorization response for any operation indicates failure, and to determine the authorization information as success when the authorization responses for the multiple operations indicate success.

[0011] In an embodiment of the disclosure, the management server component is configured to return a failure message to the management agent when the authorization information indicates failure, and to perform operation(s) according to the user operation request and return the operation result to the management agent when the authorization information indicates success.

[0012] In an embodiment of the disclosure, the network management device is used in one of a cloud environment, a software defined network (SDN) environment, and the Internet of things (IoT).

[0013] According to another aspect of the disclosure, there is provided a centralized authorization server configured with a remote authorization protocol. The centralized authorization server comprises a second reception module, an access control database, an authorization module and a second sending module. The second reception module is configured to receive a user authorization request from at least one of a plurality of network management devices configured with NETCONF protocol and located at different positions. The access control database is configured to store information about identifications and access rights of a plurality of users. The authorization module is configured to generate an authorization response for the user authorization request based on the access control database. The second sending module is configured to send the authorization response to the at least one of the plurality of network management devices.

[0014] In an embodiment of the disclosure, the information about an access right of a user comprises: an operation identification; an Xpath representing an object on which the operation is to be performed; and access control information for determining whether the user is permitted to perform the operation.

[0015] According to another aspect of the disclosure, there is provided a method at a network management device. The method comprises processing a user operation request from a management agent through NETCONF protocol. The method further comprises obtaining, for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol. Processing the user operation request is based at least on the authorization information.

[0016] In an embodiment of the disclosure, processing the user operation request comprises converting the user operation request to an operation identification and an Xpath. The Xpath represents an object on which the operation is to be performed. Obtaining the authorization information comprises sending to the centralized authorization server an authorization request including the operation identification and the Xpath. Obtaining the authorization information further comprises receiving an authorization response from the centralized authorization server. Obtaining the authorization information further comprises determining the authorization information based on the authorization response.

[0017] In an embodiment of the disclosure, there are multiple operations indicated in the user operation request. The sending of the authorization request and the receiving of the authorization response are performed iteratively for each of the multiple operations. Determining the authorization information comprises determining the authorization information as failure when the authorization response for any operation indicates failure. Determining the authorization information further comprises determining the authorization information as success when the authorization responses for the multiple operations indicate success.

[0018] In an embodiment of the disclosure, processing the user operation request comprises returning a failure message to the management agent when the authorization information indicates failure. Processing the user operation request further comprises performing operation(s) according to the user operation request when the authorization information indicates success. Processing the user operation request further comprises returning the operation result to the management agent.

[0019] According to another aspect of the disclosure, there is provided a method at a centralized authorization server configured with a remote authorization protocol. The method comprises receiving a user authorization request from at least one of a plurality of network management devices configured with NETCONF protocol and located at different positions. The method further comprises generating an authorization response for the user authorization request based on an access control database. The access control database is configured to store information about identifications and access rights of a plurality of users. The method further comprises sending the authorization response to the at least one of the plurality of network management devices.

[0020] According to another aspect of the disclosure, there is provided a method at a terminal device in a communication system. The communication system further comprises a network management device and a centralized authorization server. The method comprises sending a user operation request to the network management device through NETCONF protocol. The method further comprises receiving an operation result or a failure message from the network management device. The network management device is configured to process the user operation request through NETCONF protocol, and to obtain, for the user operation request, authorization information from the centralized authorization server through a remote authorization protocol. Processing the user operation request is based at least on the authorization information such that the operation result or the failure message is generated.

[0021] According to another aspect of the disclosure, there is provided a network management device. The network management device comprises a processor and a memory. The memory contains instructions executable by the processor, whereby the network management device is operative to process a user operation request from a management agent through NETCONF protocol. The network management device is further operative to obtain, for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol. Processing the user operation request is based at least on the authorization information.

[0022] According to another aspect of the disclosure, there is provided a network device comprising the network management device according to the above aspect.

[0023] According to another aspect of the disclosure, there is provided a centralized authorization server configured with a remote authorization protocol. The centralized authorization server comprises a processor and a memory. The memory contains instructions executable by the processor, whereby the centralized authorization server is operative to receive a user authorization request from at least one of a plurality of network management devices configured with NETCONF protocol and located at different positions. The centralized authorization server is further operative to generate an authorization response for the user authorization request based on an access control database. The access control database is configured to store information about identifications and access rights of a plurality of users. The centralized authorization server is further operative to send the authorization response to the at least one of the plurality of network management devices.

[0024] According to another aspect of the disclosure, there is provided a terminal device for use in a communication system. The communication system further comprises a network management device and a centralized authorization server. The terminal device comprises a processor and a memory. The memory contains instructions executable by the processor, whereby the terminal device is operative to

send a user operation request to the network management device through NETCONF protocol. The terminal device is further operative to receive an operation result or a failure message from the network management device. The network management device is configured to process the user operation request through NETCONF protocol, and to obtain, for the user operation request, authorization information from the centralized authorization server through a remote authorization protocol. Processing the user operation request is based at least on the authorization information such that the operation result or the failure message is generated.

[0025] According to another aspect of the disclosure, there is provided a computer program product. The computer program product comprises instructions which when executed by at least one processor, cause the at least one processor to perform the method according to the above aspect.

[0026] According to another aspect of the disclosure, there is provided a computer readable storage medium. The computer readable storage medium comprises instructions which when executed by at least one processor, cause the at least one processor to perform the method according to the above aspect.

[0027] These and other objects, features and advantages of the disclosure will become apparent from the following detailed description of illustrative embodiments thereof, which are to be read in connection with the accompanying drawings.

Brief Description of the Drawings

[0028] FIG. 1 is a block diagram showing a communication system according to an embodiment of the disclosure;

[0029] FIG. 2 is a flowchart illustrating a process according to an embodiment of the disclosure;

[0030] FIG. 3 is a flowchart illustrating a method at a network management device according to an embodiment of the disclosure;

[0031] FIG. 4 is a flowchart for explaining the method shown in FIG. 3;

[0032] FIG. 5 is a flowchart illustrating a method at a centralized authorization server according to an embodiment of the disclosure;

[0033] FIG. 6 is a flowchart illustrating a method at a terminal device according to an embodiment of the disclosure;

[0034] FIG. 7 is a block diagram showing an apparatus suitable for use in practicing some embodiments of the disclosure; and

[0035] FIG. 8 is a block diagram showing a communication system suitable for use in practicing some embodiments of the disclosure.

Detailed Description

[0036] For the purpose of explanation, details are set forth in the following description in order to provide a thorough understanding of the embodiments disclosed. It is apparent, however, to those skilled in the art that the embodiments may be implemented without these specific details or with an equivalent arrangement.

[0037] As used herein, the term "wireless communication network" refers to a network following any suitable communication standards, such as LTE-Advanced (LTE-A), LTE, Wideband Code Division Multiple Access (WCDMA), High-Speed Packet Access (HSPA), and so on. Furthermore, the communications between a terminal device and a network device in the wireless communication network may be performed according to any suitable generation communication protocols, including, but not limited to, the first generation (1G), the second generation (2G), 2.5G, 2.75G, the third generation (3G), the fourth generation (4G), 4.5G, the future fifth generation (5G) communication protocols, and/or any other protocols either currently known or to be developed in the future.

[0038] The term "network device" refers to a device in a wireless communication network via which a terminal device accesses the network and receives services therefrom. The network device refers a base station (BS), an access point (AP), a

Mobile Management Entity (MME), Multi-cell/Multicast Coordination Entity (MCE), a gateway, a server, a controller or any other suitable device in the wireless communication network. The BS may be, for example, a node B (NodeB or NB), an evolved NodeB (eNodeB or eNB), a gNB, a Remote Radio Unit (RRU), a radio header (RH), a remote radio head (RRH), a relay, a low power node such as a femto, a pico, and so forth.

[0039] Yet further examples of network device include multi-standard radio (MSR) radio equipment such as MSR BSs, network controllers such as radio network controllers (RNCs) or base station controllers (BSCs), base transceiver stations (BTSs), transmission points, transmission nodes, Multi-cell/multicast Coordination Entities (MCEs), core network nodes (e.g., MSCs, MMEs), O&M nodes, OSS nodes, SON nodes, positioning nodes (e.g., E-SMLCs), and/or MDTs. More generally, however, network device may represent any suitable device (or group of devices) capable, configured, arranged, and/or operable to enable and/or provide a terminal device access to the wireless communication network or to provide some service to a terminal device that has accessed the wireless communication network.

[0040] The term "terminal device" refers to any end device that can access a wireless communication network and receive services therefrom. By way of example and not limitation, the terminal device refers to a mobile terminal, UE, or other suitable device. The UE may be, for example, a Subscriber Station (SS), a Portable Subscriber Station, a Mobile Station (MS), or an Access Terminal (AT). The terminal device may include, but not limited to, portable computers, image capture terminal devices such as digital cameras, gaming terminal devices, music storage and playback appliances, a mobile phone, a cellular phone, a smart phone, a tablet, a wearable device, a personal digital assistant (PDA), a vehicle, and the like.

[0041] The terminal device may support device-to-device (D2D) communication, for example by implementing a 3GPP standard for sidelink communication, and may in this case be referred to as a D2D communication device.

[0042] As yet another specific example, in an Internet of Things (IOT) scenario, a terminal device may represent a machine or other device that performs monitoring and/or measurements, and transmits the results of such monitoring and/or measurements to another terminal device and/or a network equipment. The terminal device may in this case be a machine-to-machine (M2M) device, which may in a 3GPP context be referred to as a machine-type communication (MTC) device. As one particular example, the terminal device may be a UE implementing the 3GPP narrow band internet of things (NB-IoT) standard. Particular examples of such machines or devices are sensors, metering devices such as power meters, industrial machinery, or home or personal appliances, e.g. refrigerators, televisions, personal wearables such as watches etc. In other scenarios, a terminal device may represent a vehicle or other equipment that is capable of monitoring and/or reporting on its operational status or other functions associated with its operation.

[0043] In the above existing authorization solution as defined in RFC 6536, only local authorization is defined, which means there is no way to do centralized authorization for NETCONF. As a result, in the cloud/SDN environment such as the Internet of things (IoT), mobile user cannot have the integrated authorization configuration when logging in from different network access points if each user's authorization information has not been configured in every network access point. This may remarkably slow down the network provisioning performance especially in the provisioning of massive devices with large individual authorization configurations.

[0044] The present disclosure proposes a centralized authorization solution for NETCONF. Hereinafter, the solution will be described in detail with reference to FIGs. 1-8.

[0045] FIG. 1 is a block diagram showing a communication system according to an embodiment of the disclosure. The communication system may be part of a cloud/SDN environment such as the Internet of things (IoT). As shown, the communication system comprises a network management device 12, a management agent 14 and a centralized authorization server 16. The network management device

12 comprises a management server component 122 and an authorization client component 124. The management server component 122 is configured, with NETCONF protocol, to process a user operation request from the management agent 14 based at least on authorization information from the authorization client component 124. Correspondingly, the management agent 14 is configured, with NETCONF protocol, to send the user operation request to and receive the operation result from the management server component 122.

[0046] The authorization client component 124 is configured, with a remote authorization protocol, to obtain, for the user operation request, the authorization information from the centralized authorization server 16. Correspondingly, the centralized authorization server 16 is configured, with the same remote authorization protocol, to generate an authorization response for the authorization client component 124. As an example, the remote authorization protocol may be terminal access controller access-control system plus (TACACS+) protocol, which can provide an extensible architecture of doing authorization. Alternatively, any other suitable remote authorization protocols such as remote authentication dial in user service (RADIUS) protocol may be employed.

[0047] In this way, the above solution can provide a way to do NETCONF centralized authorization. In turn, it can provide the possibility of doing centralized access-right control for a group of network management devices within the control of this solution. As an exemplary example, in the IoT case, the network management device 12 may be a gateway for access to a home network. The management agent 14 may be embedded in a terminal device or may be a terminal device itself, such as a mobile phone, a pad computer, a laptop computer, a desktop computer, or any other devices (e.g., a vehicle) with wired and/or wireless communication capability. The centralized authorization server 16 may be a remote server serving a plurality of the gateways located at different positions. This can easily provide the integrated authorization information without requiring the gateways in different positions to have the same authorization configuration. As another exemplary example, the network management

device 12 may be a gateway for access to the Internet of vehicles (IoV). The management agent 14 may be embedded in a vehicle or may be a vehicle itself. The centralized authorization server 16 may be a remote server serving a plurality of the gateways located at different positions. In this case, the authorization response may be generated for a vehicle according to the vehicle's location.

[0048] As shown, the authorization client component 124 may comprise a first sending module 1242, a first reception module 1244 and a determination module 1246. The centralized authorization server 16 may comprise a second reception module 162, an access control database 164, an authorization module 166 and a second sending module 168. The implementing details of the above constituent parts of the communication system will be described in detail with reference to FIG. 2.

[0049] FIG. 2 is a flowchart illustrating a process according to an embodiment of the disclosure. Although the process is described in the context of the IoT, those skilled in the art will understand that the principle of the present disclosure may also be applied to any other scenarios in which centralized authorization is needed for NETCONF.

[0050] At block 202, a user starts a session via the management agent 14. As described above, the management agent 14 is a NETCONF agent which may be embedded in a terminal device. The user may operate the terminal device to trigger the start of the session. The session may be a secure shell (SSH) session. It may be started by sending an initial transmission control protocol (TCP) connection request from the management agent 14 to the management server component 122.

[0051] At block 204, the session is established between the management agent 14 and the management server component 122. Specifically, in response to the initial TCP connection request, the management server component 122 may negotiate the SSH protocol version and exchange keys for message integrity and encryption with the management agent 14. Then, the management agent 14 may send an authentication request to the management server component 122. Various authentication protocols such as RADIUS protocol may be used to authenticate the user. Once the user has

been successfully authenticated, the management agent 14 may send a session request to the management server component 122 such that the SSH session is established.

[0052] At block 206, the user sends an operation request to the management server component 122 via the management agent 14. The operation request may be sent via remote procedure call (RPC). The operation request is expressed in extensible markup language (XML) and may indicate one or more operations.

[0053] In response to the operation request, transaction processing is started. Specifically, at block 208, the management server component 122 converts the operation request to an operation identification and an Xpath. This may be achieved by a conversion from XML to Xpath. The operation identification may be the name of an executive program for performing an operation, such as "get-config", "edit-config" or the like as defined in NETCONF. The Xpath may represent an object on which the operation is to be performed. Since there may be one or more operations indicated in the operation request, one or more pairs of operation identifications and Xpaths may be obtained.

[0054] At block 210, the management server component 122 passes the one or more pairs of operation identifications and Xpaths to the authorization client component 124. At block 212, the authorization client component 124 (specifically, the first sending module 1242) sends to the centralized authorization server 16 (specifically, the second reception module 162) an authorization request including the one or more pairs of operation identifications and Xpaths. The authorization request further comprises an identification of the user, such as user name, group name or the like, which may be determined during the authentication performed at block 204. For example, each pair of operation identification and Xpath may be set as two arguments in the Authorization_REQUEST message in the case where TACACS+ protocol is used.

[0055] In response to the authorization request, the centralized authorization server 16 (specifically, the authorization module 166 together with the access control database 164) generates one or more authorization responses at block 214. The access control

database 164 is configured to store information about identifications and access rights of a plurality of users. The information about an access right of a user may include: an operation identification; an Xpath representing an object on which the operation is to be performed; and access control information for determining whether the user is permitted to perform the operation. The access control information may include an access control rule for specifying whether a user name or a group name has an access right for particular operation(s).

[0056] As an exemplary example, a model for the access control database 164 may be represented as follows:

```
+--rw groups
      | +--rw group [name]
      |    +--rw name        group-name-type
      |    +--rw user-name*   user-name-type
      +--rw rule-list [name]
        +--rw name     string
        +--rw group*   union
        +--rw rule [name]
          +--rw name                string
          +--rw Xpath               string
          +--rw access-operations?  union
          +--rw action              action-type
          +--rw comment?            String
```

[0057] In the IoT case such as home-appliance access control scenario, the above model may be specifically represented as follows:

```
{
   "groups": {
       "group"              : [
       {
        "name"              :  "admin-group",
        "user-name"           :  ["admin", "parent"]
       },
       {
```

```
        "name"          : "user-group",
        "user-name"     : ["child"]
      }
      ]
  },
  "rule-list"           : [
      {
        "name"          : "admin-rules"
        "group"         : "admin-group"
        "rule"          : [
        {
          "name"        : "admin-rule-1",
          "Xpath"       : "/home/appliance/",
          "access-operations"  : "*",
          "action"      : "permit",
          "comment"     : "Admin permits all operation"
        }
        ]
      },
      {
        "name"          : "user-rules"
        "group"         : "user-group"
        "rule"          : [
        {
          "name"        : "user-rule-1",
          "Xpath"       : "/home/appliance/",
          "access-operations"  : "*",
          "action"      : "deny",
          "comment"     : "Deny all operation by default"
        }'
        {
          "name"        : "user-rule-2",
          "Xpath"       : "/home/appliance/",
          "access-operations"  : "read",
          "action"      : "permit",
          "comment"     : "Permit reading"
        }
        ]
      },
      ]
}
```

[0058] The authorization module 166 is configured to generate an authorization response for the authorization request based on the access control database 164. For example, the corresponding access control rule(s) may be located from the access control database 164 according to the user identification and be processed to determine the authorization response. In the above instance of home-appliance access control, if the user name is "child" and the requested operation is "read"+"/home/appliance/", then the rule "user-rule-2" may be located and processed such that the authorization response is determined as success.

[0059] It should be noted that the present disclosure is not limited to the above examples. Any features related to the access control as defined in NETCONF protocols such as RFC6536 may be employed in the access control database 164 and the authorization module 166. In this way, new authorization attributes containing, for example, the NETCONF Xpath and the corresponding access-right are introduced into the remote authorization protocol between the authorization client component 124 and the centralized authorization server 16.

[0060] At block 216, the centralized authorization server 16 (specifically, the second sending module 168) sends the generated authorization response to the authorization client component 124 (specifically, the first reception module 1244). For example, the authorization response may be set into the status field of the Authorization_RESPONSE message in the case where TACACS+ protocol is used. Note that in the case where multiple operations are indicated in the operation request, blocks 212, 214 and 216 may be performed iteratively for each of the multiple operations.

[0061] At block 218, the authorization client component 124 (specifically, the determination module 1246) determines the authorization information based on the one or more authorization responses. For example, in the case where multiple operations are indicated in the operation request, the authorization information may be determined as failure if the authorization response for any operation indicates failure, and may be determined as success if the authorization responses for all the operations

indicate success. At block 220, the authorization client component 124 (specifically, the determination module 1246) passes the authorization information to the management server component 122.

[0062] At block 222, the management server component 122 generates the operation result according to the authorization information. If the authorization information indicates failure, the result may be generated to indicate failure. On the other hand, if the authorization information indicates success, the executive program(s) may be run by means of a YANG base database to perform the one or more operations. At block 224, the result is returned from the management server component 122 to the management agent 14.

[0063] FIG. 3 is a flowchart illustrating a method at a network management device according to an embodiment of the disclosure. At block 302, the network management device processes a user operation request from a management agent through NETCONF protocol. At block 304, the network management device obtains, for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol. The processing of the user operation request at block 302 is based at least on the authorization information.

[0064] FIG. 4 is a flowchart for explaining the method shown in FIG. 3. For example, block 302 may be implemented as blocks 406 and 412-418 shown in FIG. 4. Block 304 may be implemented as blocks 408 and 410 shown in FIG. 4. At block 406, the user operation request is converted to an operation identification and an Xpath. The Xpath represents an object on which the operation is to be performed. Block 406 may correspond to block 208 shown in FIG. 2.

[0065] At block 408, an authorization request including the operation identification and the Xpath is sent to the centralized authorization server. Block 408 may correspond to block 212 shown in FIG. 2. At block 410, an authorization response is received from the centralized authorization server. Block 410 may correspond to block 216 shown in FIG. 2.

[0066] At block 412, the authorization information is determined based on the authorization response. Block 412 may correspond to block 218 shown in FIG. 2. At block 414, a failure message is returned to the management agent when the authorization information indicates failure. On the other hand, at block 416, operation(s) are performed according to the user operation request when the authorization information indicates success. At block 418, the operation result is returned to the management agent. Blocks 414-418 may correspond to blocks 222 and 224 shown in FIG. 2.

[0067] FIG. 5 is a flowchart illustrating a method at a centralized authorization server according to an embodiment of the disclosure. The centralized authorization server is configured with a remote authorization protocol. At block 502, a user authorization request is received from at least one of a plurality of network management devices configured with NETCONF protocol and located at different positions. Block 502 may correspond to block 212 shown in FIG. 2.

[0068] At block 504, an authorization response is generated for the user authorization request based on an access control database. The access control database is configured to store information about identifications and access rights of a plurality of users. Block 504 may correspond to block 214 shown in FIG. 2. At block 506, the authorization response is sent to the at least one of the plurality of network management devices. Block 506 may correspond to block 216 shown in FIG. 2. It should be noted that two steps shown in succession may, in fact, be executed substantially concurrently, or the steps may sometimes be executed in the reverse order, depending upon the functionality involved.

[0069] FIG. 6 is a flowchart illustrating a method at a terminal device in a communication system according to an embodiment of the disclosure. The communication system further comprises a network management device and a centralized authorization server, as shown in FIG. 2. At block 602, a user operation request is sent to the network management device through NETCONF protocol. Block 602 may correspond to block 206 shown in FIG. 2. As described above, the network

management device is configured to process the user operation request through NETCONF protocol, and to obtain, for the user operation request, authorization information from the centralized authorization server through a remote authorization protocol. Processing the user operation request is based at least on the authorization information such that an operation result or a failure message is generated. At block 604, the operation result or the failure message is received from the network management device. Block 604 may correspond to block 224 shown in FIG. 2.

[0070] FIG. 7 is a block diagram showing an apparatus suitable for use in practicing some embodiments of the disclosure. For example, any one of the terminal device (embedded with the management agent 14), the network management device 12 and the centralized authorization server 16 may be implemented through the apparatus 700. As shown, the apparatus 700 may include a processor 710, a memory 720 that stores a program, and a communication interface 730 for communicating data with other external devices through wired and/or wireless communication.

[0071] The program is assumed to include program instructions that, when executed by the processor 710, enable the apparatus 700 to operate in accordance with the embodiments of the present disclosure, as discussed above. That is, the embodiments of the present disclosure may be implemented at least in part by computer software executable by the processor 710, or by hardware, or by a combination of software and hardware.

[0072] The memory 720 may be of any type suitable to the local technical environment and may be implemented using any suitable data storage technology, such as semiconductor based memory devices, flash memory, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory. The processor 710 may be of any type suitable to the local technical environment, and may include one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multi-core processor architectures, as non-limiting examples.

[0073] FIG. 8 is a block diagram showing a communication system suitable for use in practicing some embodiments of the disclosure. In this example, the terminal device is implemented as a user equipment (UE) which can communicate, via at least a cellular base station, with the network management device which is implemented as a host computer. Similar to the network management device, the centralized authorization server may also be implemented as a host computer. Note that the centralized authorization server is omitted in communication system 800 of FIG. 8 for brevity.

[0074] In other words, the present disclosure provides a communication system which comprises a UE, a base station, a first host computer and a second host computer. The first host computer includes a first processing circuitry and a first communication interface which are configured to act as the network management device. The second host computer includes a second processing circuitry and a second communication interface which are configured to act as the centralized authorization server. The first communication interface is configured to communicate with a cellular network. The cellular network comprises the base station having a radio interface and a third processing circuitry. The third processing circuitry is configured to transfer a user operation request from the UE to the first host computer and transfer an operation result or a failure message from the first host computer to the UE.

[0075] Specifically, in communication system 800, host computer 810 comprises hardware 815 including communication interface 816 configured to set up and maintain a wired or wireless connection with an interface of a different communication device of communication system 800. Host computer 810 further comprises processing circuitry 818, which may have storage and/or processing capabilities. In particular, processing circuitry 818 may comprise one or more programmable processors, application-specific integrated circuits, field programmable gate arrays or combinations of these (not shown) adapted to execute instructions. Host computer 810 further comprises software 811, which is stored in or accessible by host computer 810 and executable by processing circuitry 818. Software 811 includes host application 812. Host application 812 may be operable to provide a service to a

remote user, such as UE 830 connecting via connection 850 terminating at UE 830 and host computer 810. In providing the service to the remote user, host application 812 may provide user data which is transmitted using connection 850.

[0076] Communication system 800 further includes base station 820 provided in a telecommunication system and comprising hardware 825 enabling it to communicate with host computer 810 and with UE 830. Hardware 825 may include communication interface 826 for setting up and maintaining a wired or wireless connection with an interface of a different communication device of communication system 800, as well as radio interface 827 for setting up and maintaining at least wireless connection 870 with UE 830 located in a coverage area (not shown in Figure 8) served by base station 820. Communication interface 826 may be configured to facilitate connection 860 to host computer 810. Connection 860 may be direct or it may pass through a core network (not shown in Figure 8) of the telecommunication system and/or through one or more intermediate networks outside the telecommunication system. In the embodiment shown, hardware 825 of base station 820 further includes processing circuitry 828, which may comprise one or more programmable processors, application-specific integrated circuits, field programmable gate arrays or combinations of these (not shown) adapted to execute instructions. Base station 820 further has software 821 stored internally or accessible via an external connection.

[0077] Communication system 800 further includes UE 830 already referred to. Its hardware 835 may include radio interface 837 configured to set up and maintain wireless connection 870 with a base station serving a coverage area in which UE 830 is currently located. Hardware 835 of UE 830 further includes processing circuitry 838, which may comprise one or more programmable processors, application-specific integrated circuits, field programmable gate arrays or combinations of these (not shown) adapted to execute instructions. UE 830 further comprises software 831, which is stored in or accessible by UE 830 and executable by processing circuitry 838. Software 831 includes client application 832. Client application 832 may be operable to provide a service to a human or non-human user via UE 830, with the support of

host computer 810. In host computer 810, an executing host application 812 may communicate with the executing client application 832 via connection 850 terminating at UE 830 and host computer 810. In providing the service to the user, client application 832 may receive request data from host application 812 and provide user data in response to the request data. Connection 850 may transfer both the request data and the user data. Client application 832 may interact with the user to generate the user data that it provides.

[0078] In FIG. 8, connection 850 has been drawn abstractly to illustrate the communication between host computer 810 and UE 830 via base station 820, without explicit reference to any intermediary devices and the precise routing of messages via these devices. Network infrastructure may determine the routing, which it may be configured to hide from UE 830 or from the service provider operating host computer 810, or both. While connection 850 is active, the network infrastructure may further take decisions by which it dynamically changes the routing (e.g., on the basis of load balancing consideration or reconfiguration of the network).

[0079] In general, the various exemplary embodiments may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. For example, some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device, although the disclosure is not limited thereto. While various aspects of the exemplary embodiments of this disclosure may be illustrated and described as block diagrams, flow charts, or using some other pictorial representation, it is well understood that these blocks, apparatus, systems, techniques or methods described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

[0080] As such, it should be appreciated that at least some aspects of the exemplary embodiments of the disclosure may be practiced in various components such as

integrated circuit chips and modules. It should thus be appreciated that the exemplary embodiments of this disclosure may be realized in an apparatus that is embodied as an integrated circuit, where the integrated circuit may comprise circuitry (as well as possibly firmware) for embodying at least one or more of a data processor, a digital signal processor, baseband circuitry and radio frequency circuitry that are configurable so as to operate in accordance with the exemplary embodiments of this disclosure.

[0081] It should be appreciated that at least some aspects of the exemplary embodiments of the disclosure may be embodied in computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by a processor in a computer or other device. The computer executable instructions may be stored on a computer readable medium such as a hard disk, optical disk, removable storage media, solid state memory, RAM, etc. As will be appreciated by one of skill in the art, the function of the program modules may be combined or distributed as desired in various embodiments. In addition, the function may be embodied in whole or in part in firmware or hardware equivalents such as integrated circuits, field programmable gate arrays (FPGA), and the like.

[0082] References in the present disclosure to “one embodiment”, “an embodiment” and so on, indicate that the embodiment described may include a particular feature, structure, or characteristic, but it is not necessary that every embodiment includes the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0083] It should be understood that, although the terms “first”, “second” and so on may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, a first element could be termed a second element, and similarly, a second element could be termed a first element, without departing from the scope of the disclosure. As used herein, the term “and/or” includes any and all combinations of one or more of the associated listed terms.

[0084] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the present disclosure. As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises”, “comprising”, “has”, “having”, “includes” and/or “including”, when used herein, specify the presence of stated features, elements, and/or components, but do not preclude the presence or addition of one or more other features, elements, components and/ or combinations thereof. The terms “connect”, “connects”, “connecting” and/or “connected” used herein cover the direct and/or indirect connection between two elements.

[0085] The present disclosure includes any novel feature or combination of features disclosed herein either explicitly or any generalization thereof. Various modifications and adaptations to the foregoing exemplary embodiments of this disclosure may become apparent to those skilled in the relevant arts in view of the foregoing description, when read in conjunction with the accompanying drawings. However, any and all modifications will still fall within the scope of the non-Limiting and exemplary embodiments of this disclosure.

Claims

What is claimed is:

1. A network management device (12) comprising:

a management server component (122) configured, with network configuration (NETCONF) protocol, to process a user operation request from a management agent (14) based at least on authorization information from an authorization client component (124); and

the authorization client component (124) configured, with a remote authorization protocol, to obtain, for the user operation request, the authorization information from a centralized authorization server (16).

2. The network management device (12) according to claim 1, wherein the remote authorization protocol is terminal access controller access-control system plus (TACACS+) protocol or remote authentication dial in user service (RADIUS) protocol.

3. The network management device (12) according to claim 1 or 2, wherein the management server component (122) is configured to convert the user operation request to an operation identification and an Xpath, wherein the Xpath represents an object on which the operation is to be performed; and

wherein the authorization client component (124) comprises:

a first sending module (1242) configured to send to the centralized authorization server (16) an authorization request including the operation identification and the Xpath;

a first reception module (1244) configured to receive an authorization response from the centralized authorization server (16); and

a determination module (1246) configured to determine the authorization information based on the authorization response.

4. The network management device (12) according to claim 3, wherein there are multiple operations indicated in the user operation request;

wherein the first sending module (1242) and the first reception module (1244) operate iteratively for each of the multiple operations; and

wherein the determination module (1246) is configured to determine the authorization information as failure when the authorization response for any operation indicates failure, and to determine the authorization information as success when the authorization responses for the multiple operations indicate success.

5. The network management device (12) according to any of claims 1 to 4, wherein the management server component (122) is configured to return a failure message to the management agent (14) when the authorization information indicates failure, and to perform operation(s) according to the user operation request and return the operation result to the management agent (14) when the authorization information indicates success.

6. The network management device (12) according to any of claims 1 to 5, wherein the network management device (12) is used in one of a cloud environment, a software defined network (SDN) environment, and the Internet of things (IoT).

7. A centralized authorization server (16) configured with a remote authorization protocol, the centralized authorization server (16) comprising:

a second reception module (162) configured to receive a user authorization request from at least one (12) of a plurality of network management devices configured with network configuration (NETCONF) protocol and located at different positions;

an access control database (164) configured to store information about identifications and access rights of a plurality of users;

an authorization module (166) configured to generate an authorization response for the user authorization request based on the access control database (164); and

a second sending module (168) configured to send the authorization response to the at least one (12) of the plurality of network management devices.

8. The centralized authorization server (16) according to claim 7, wherein the remote authorization protocol is terminal access controller access-control system plus (TACACS+) protocol or remote authentication dial in user service (RADIUS) protocol.

9. The centralized authorization server (16) according to claim 7 or 8, wherein the information about an access right of a user comprises:

an operation identification;

an Xpath representing an object on which the operation is to be performed; and

access control information for determining whether the user is permitted to perform the operation.

10. A method at a network management device, the method comprising:

processing (302) a user operation request from a management agent through network configuration (NETCONF) protocol; and

obtaining (304), for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol;

wherein processing (302) the user operation request is based at least on the authorization information.

11. The method according to claim 10, wherein processing (302) the user operation request comprises converting (406) the user operation request to an

operation identification and an Xpath, wherein the Xpath represents an object on which the operation is to be performed; and

wherein obtaining (304) the authorization information comprises:

sending (408) to the centralized authorization server an authorization request including the operation identification and the Xpath;

receiving (410) an authorization response from the centralized authorization server; and

determining (412) the authorization information based on the authorization response.

12. The method according to claim 11, wherein there are multiple operations indicated in the user operation request;

wherein the sending (408) of the authorization request and the receiving (410) of the authorization response are performed iteratively for each of the multiple operations; and

wherein determining (412) the authorization information comprises:

determining the authorization information as failure when the authorization response for any operation indicates failure; and

determining the authorization information as success when the authorization responses for the multiple operations indicate success.

13. The method according to any of claims 10 to 12, wherein processing (302) the user operation request comprises:

returning (414) a failure message to the management agent when the authorization information indicates failure;

performing (416) operation(s) according to the user operation request when the authorization information indicates success; and

returning (418) the operation result to the management agent.

14. A method at a centralized authorization server configured with a remote authorization protocol, the method comprising:

receiving (502) a user authorization request from at least one of a plurality of network management devices configured with network configuration (NETCONF) protocol and located at different positions;

generating (504) an authorization response for the user authorization request based on an access control database, wherein the access control database is configured to store information about identifications and access rights of a plurality of users; and

sending (506) the authorization response to the at least one of the plurality of network management devices.

15. The method according to claim 14, wherein the information about an access right of a user comprises:

an operation identification;

an Xpath representing an object on which the operation is to be performed; and

access control information for determining whether the user is permitted to perform the operation.

16. A method at a terminal device in a communication system, wherein the communication system further comprises a network management device and a centralized authorization server, the method comprising:

sending (602) a user operation request to the network management device through network configuration (NETCONF) protocol; and

receiving (604) an operation result or a failure message from the network management device;

wherein the network management device is configured to process the user operation request through NETCONF protocol, and to obtain, for the user operation request, authorization information from the centralized authorization server through a remote authorization protocol; and

wherein processing the user operation request is based at least on the authorization information such that the operation result or the failure message is generated.

17. A network management device (700) comprising:

a processor (710); and

a memory (720), the memory (720) containing instructions executable by the processor (710), whereby the network management device (700) is operative to:

process (302) a user operation request from a management agent through network configuration (NETCONF) protocol; and

obtain (304), for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol;

wherein processing (302) the user operation request is based at least on the authorization information.

18. The network management device (700) according to claim 17, wherein the network management device (700) is operative to perform the method of any of claims 11 to 13.

19. A network device comprising the network management device (700) according to claim 17 or 18.

20. A centralized authorization server (700) configured with a remote authorization protocol, the centralized authorization server (700) comprising:

a processor (710); and

a memory (720), the memory (720) containing instructions executable by the processor (710), whereby the centralized authorization server (700) is operative to:

receive (502) a user authorization request from at least one of a plurality of network management devices configured with network configuration (NETCONF) protocol and located at different positions;

generate (504) an authorization response for the user authorization request based on an access control database, wherein the access control database is configured to store information about identifications and access rights of a plurality of users; and

send (506) the authorization response to the at least one of the plurality of network management devices.

21. The centralized authorization server (700) according to claim 20, wherein the information about an access right of a user comprises:

an operation identification;

an Xpath representing an object on which the operation is to be performed; and

access control information for determining whether the user is permitted to perform the operation.

22. A terminal device (700) for use in a communication system, wherein the communication system further comprises a network management device and a centralized authorization server, the terminal device (700) comprising:

a processor (710); and

a memory (720), the memory (720) containing instructions executable by the processor (710), whereby the terminal device (700) is operative to:

send (602) a user operation request to the network management device through network configuration (NETCONF) protocol; and

receive (604) an operation result or a failure message from the network management device;

wherein the network management device is configured to process the user operation request through NETCONF protocol, and to obtain, for the user operation request, authorization information from the centralized authorization server through a remote authorization protocol; and

wherein processing the user operation request is based at least on the authorization information such that the operation result or the failure message is generated.

23. A computer program product comprising instructions which when executed by at least one processor, cause the at least one processor to perform the method according to any of claims 10 to 16.

24. A computer readable storage medium comprising instructions which when executed by at least one processor, cause the at least one processor to perform the method according to any of claims 10 to 16.

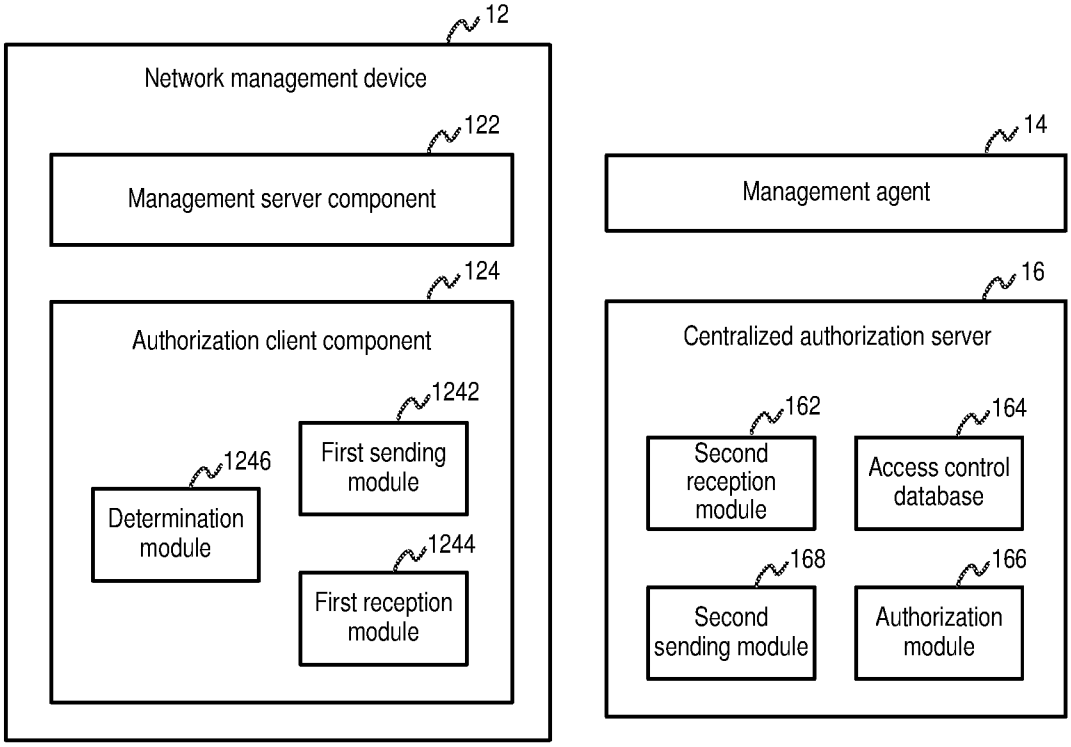
12
Network management device
122
Management server component
124
Authorization client component
1242
First sending module
1246
Determination module
1244
First reception module
14
Management agent
16
Centralized authorization server
162
Second reception module
164
Access control database
168
Second sending module
166
Authorization module

FIG. 1

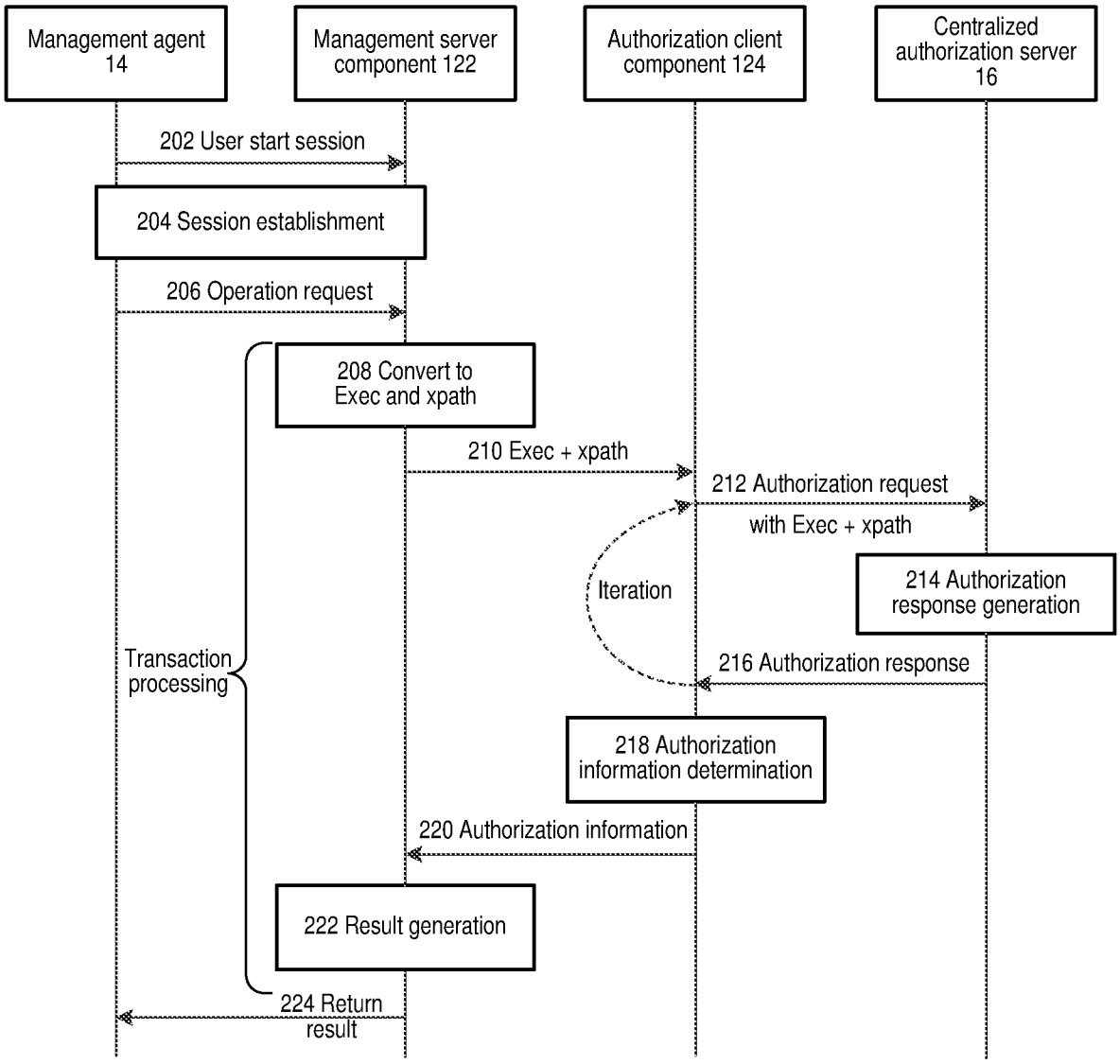
Management agent 14
Management server component 122
Authorization client component 124
Centralized authorization server 16
202 User start session
204 Session establishment
206 Operation request
208 Convert to Exec and xpath
210 Exec + xpath
212 Authorization request with Exec + xpath
Iteration
214 Authorization response generation
Transaction processing
216 Authorization response
218 Authorization information determination
220 Authorization information
222 Result generation
224 Return result

FIG. 2

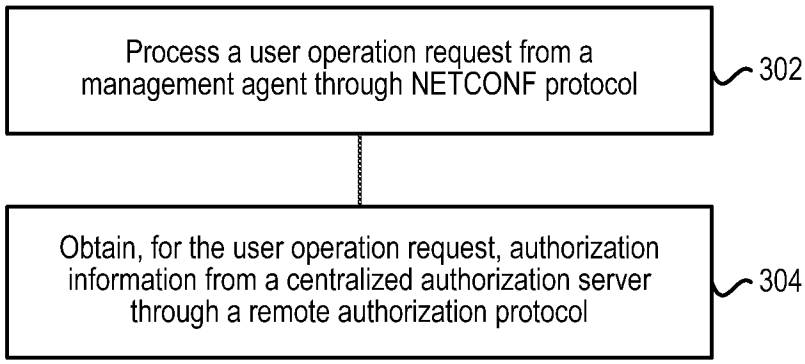
Process a user operation request from a management agent through NETCONF protocol
302
Obtain, for the user operation request, authorization information from a centralized authorization server through a remote authorization protocol
304

FIG. 3

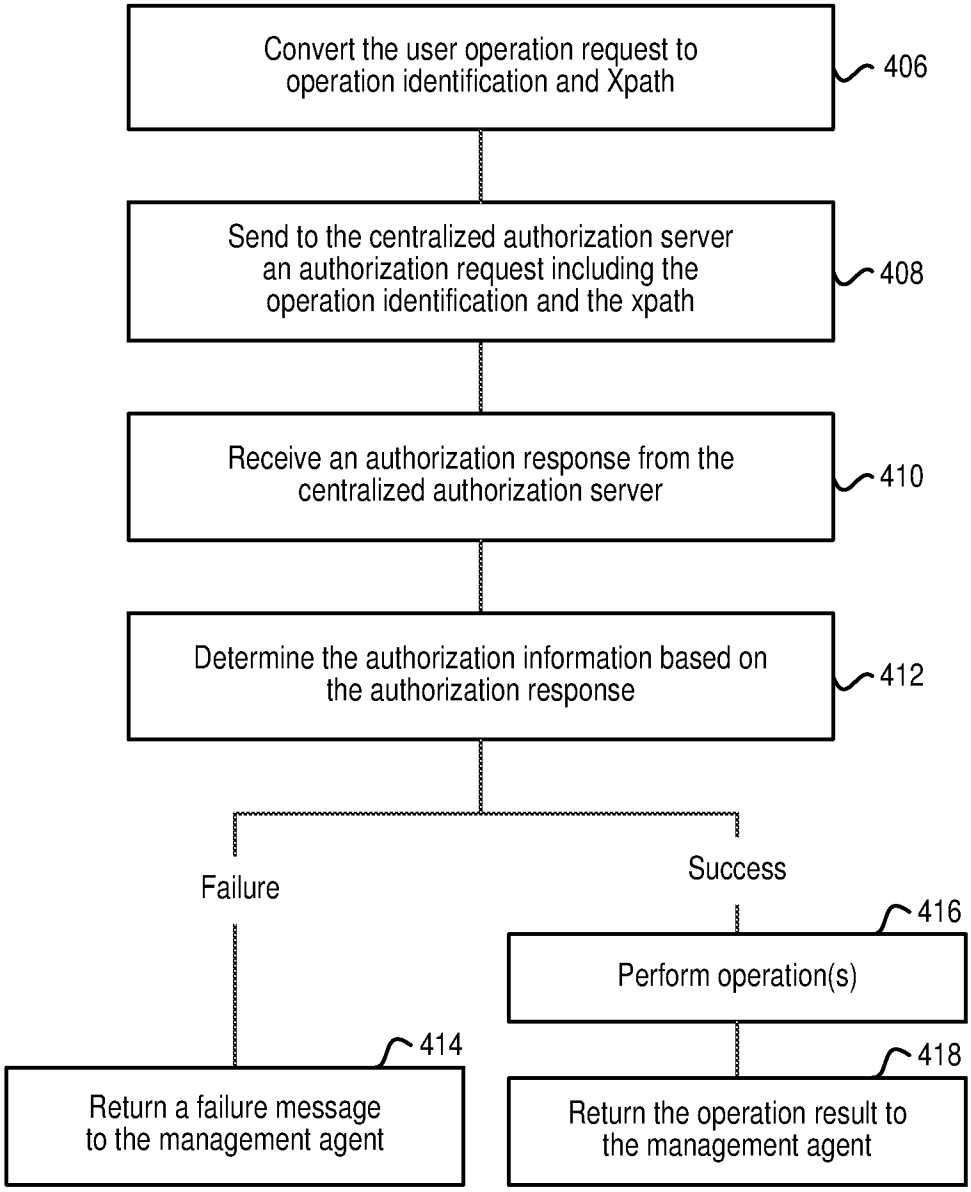
Convert the user operation request to operation identification and Xpath
406
Send to the centralized authorization server an authorization request including the operation identification and the xpath
408
Receive an authorization response from the centralized authorization server
410
Determine the authorization information based on the authorization response
412
Failure
Success
416
Perform operation(s)
414
Return a failure message to the management agent
418
Return the operation result to the management agent

FIG. 4

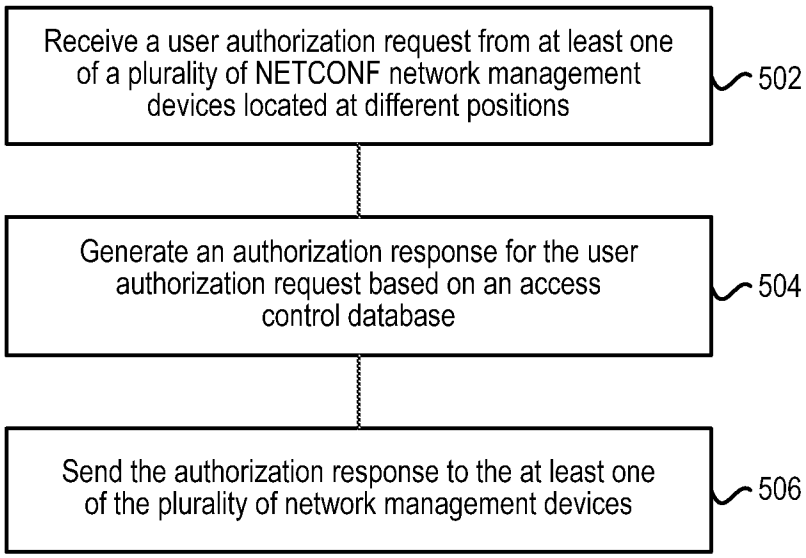
Receive a user authorization request from at least one of a plurality of NETCONF network management devices located at different positions
502
Generate an authorization response for the user authorization request based on an access control database
504
Send the authorization response to the at least one of the plurality of network management devices
506

FIG. 5

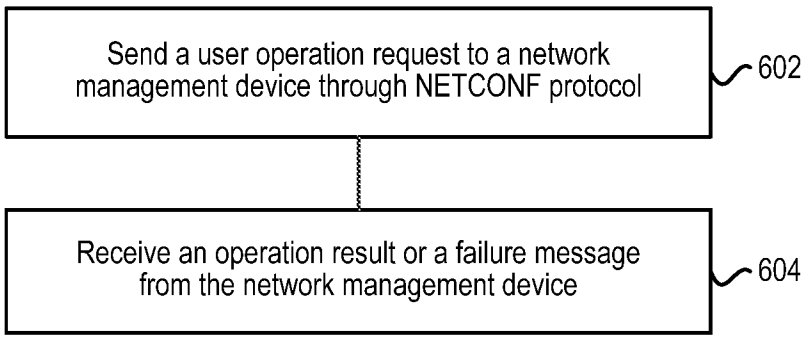
Send a user operation request to a network management device through NETCONF protocol
602
Receive an operation result or a failure message from the network management device
604

FIG. 6

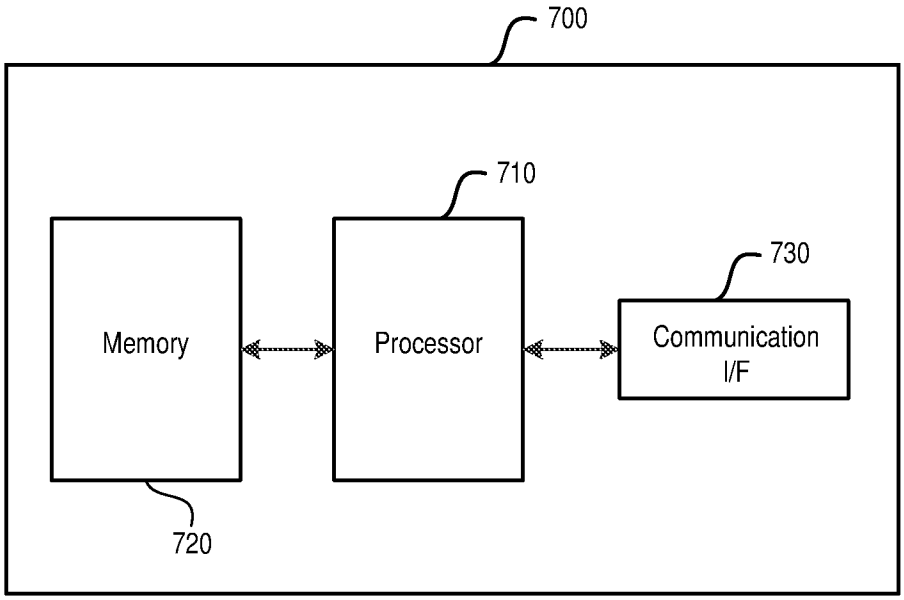
700
710
730
Memory
Processor
Communication I/F
720

FIG. 7

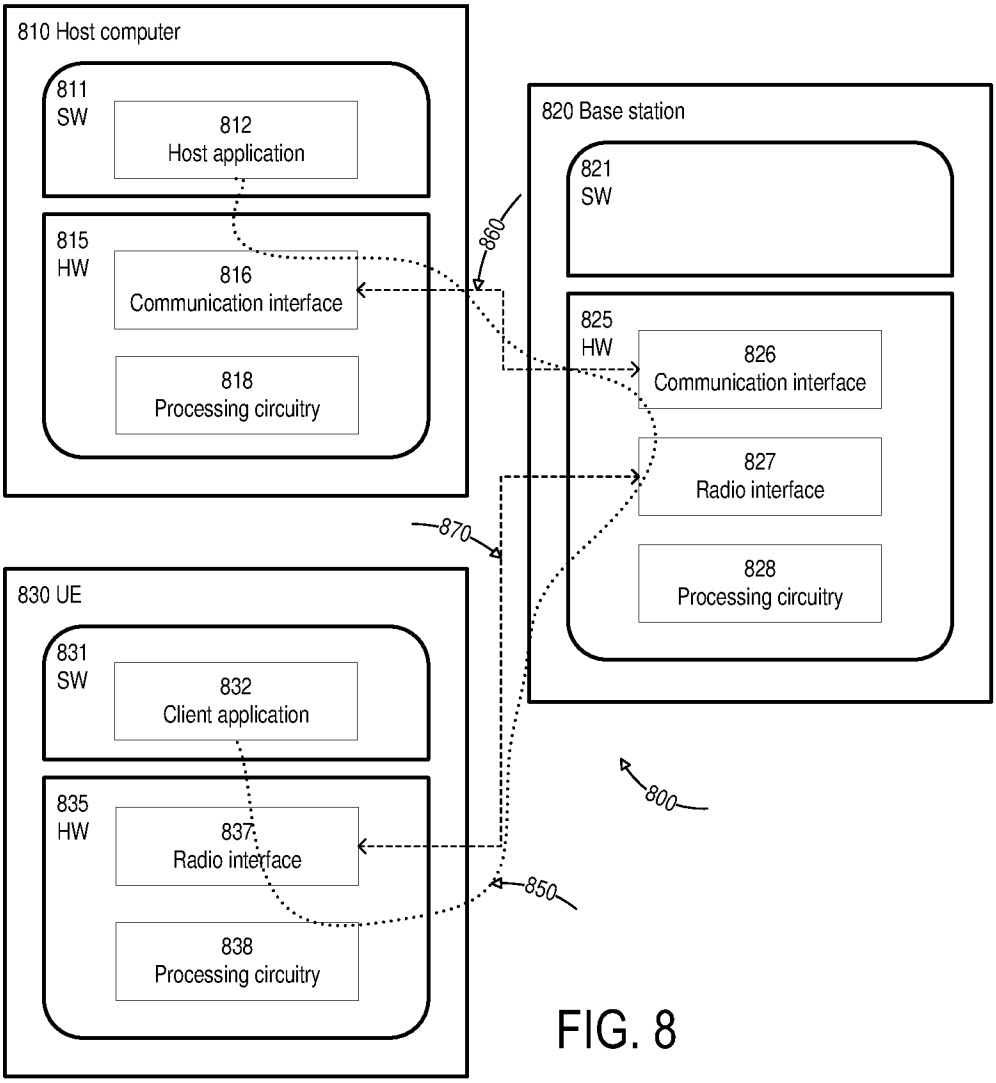
810 Host computer
811 SW
812 Host application
815 HW
816 Communication interface
818 Processing circuitry
820 Base station
821 SW
825 HW
826 Communication interface
827 Radio interface
828 Processing circuitry
860
870
830 UE
831 SW
832 Client application
835 HW
837 Radio interface
838 Processing circuitry
850
800

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/114458

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W

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

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

CNTXT;CPRSABS;CNKI;VEN;USTXT;EPTXT;WOTXT: NETCONF,authoriz+,authenticat+,server?,radius,AAA,centraliz+, request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008056161 A1 (HITACHI LTD) 06 March 2008 (2008-03-06) description, paragraphs [0056]-[0064], [0189]	1-24
A	CN 101237443 A (HUAWEI TECH CO LTD) 06 August 2008 (2008-08-06) the whole document	1-24
A	CN 105765921 A (ORACLE INT CORP) 13 July 2016 (2016-07-13) the whole document	1-24
A	CN 106454823 A (CHINA SOUTHERN POWER GRID CO) 22 February 2017 (2017-02-22) the whole document	1-24

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 August 2018	**31 August 2018**

Name and mailing address of the ISA/CN	Authorized officer
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**YU,Ruifu**
Facsimile No. **(86-10)62019451**	Telephone No. **86-010-62411248**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/114458

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2008056161	A1	06 March 2008	JP	2008060692	A	13 March 2008
				JP	4714111	B2	29 June 2011
				US	7826393	B2	02 November 2010
CN	101237443	A	06 August 2008	US	2009300743	A1	03 December 2009
				EP	2106089	B1	10 May 2017
				EP	2106089	A4	17 July 2013
				US	8276194	B2	25 September 2012
				WO	2008095444	A1	14 August 2008
				CN	101237443	B	22 August 2012
				EP	2106089	A1	30 September 2009
CN	105765921	A	13 July 2016	JP	2017503387	A	26 January 2017
				US	2015149656	A1	28 May 2015
				EP	3075108	A1	05 October 2016
				WO	2015080906	A1	04 June 2015
CN	106454823	A	22 February 2017		None		