US 20210006556A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2021/0006556 A1

He et al. (43) Pub. Date: Jan. 7, 2021

(54) **FORWARDING METHOD, FORWARDING APPARATUS, AND FORWARDER FOR AUTHENTICATION INFORMATION IN INTERNET OF THINGS**

(71) Applicant: **Huawei Technologies Co., Ltd.**, Shenzhen (CN)

(72) Inventors: **Danping He**, Shenzhen (CN); **Dacheng Zhang**, Shenzhen (CN)

(21) Appl. No.: **17/031,061**

(22) Filed: **Sep. 24, 2020**

Related U.S. Application Data

(63) Continuation of application No. 15/639,248, filed on Jun. 30, 2017, which is a continuation of application No. PCT/CN2015/096300, filed on Dec. 3, 2015.

(30) **Foreign Application Priority Data**

Jan. 4, 2015 (CN) 201510003726.5

Publication Classification

(51) **Int. Cl.**

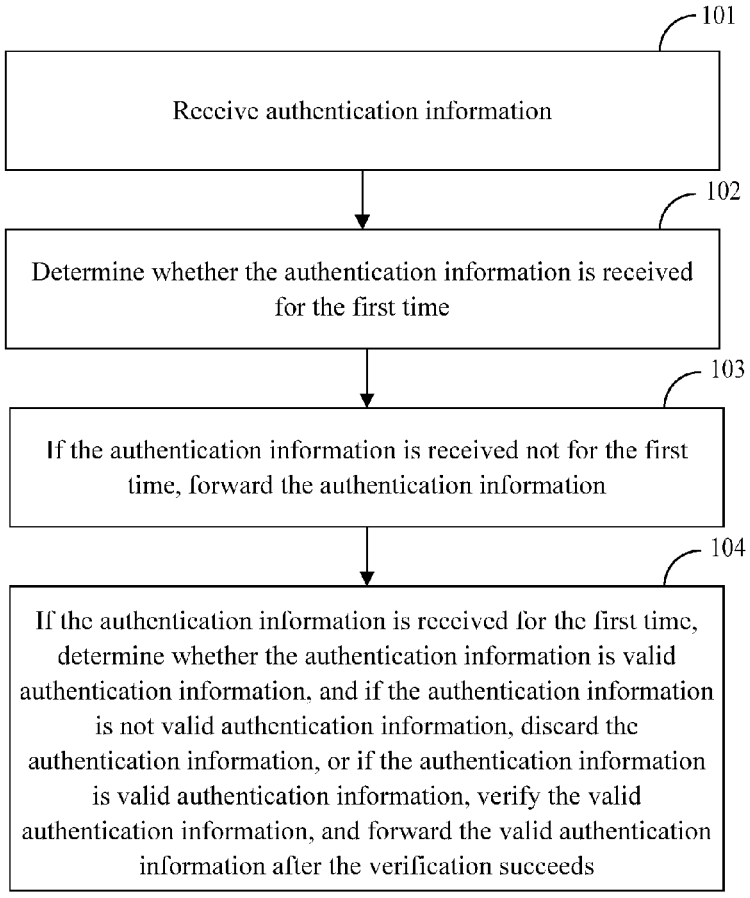
H04L 29/06	(2006.01)
H04W 12/06	(2006.01)
H04W 12/12	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/0853*** (2013.01); ***H04L 29/06*** (2013.01); ***H04L 63/1441*** (2013.01); ***H04W 12/06*** (2013.01); ***H04L 63/0884*** (2013.01); *H04L 2463/142* (2013.01); ***H04W 12/1205*** (2019.01); ***H04L 63/083*** (2013.01); ***H04L 63/126*** (2013.01); *H04L 63/108* (2013.01); *H04L 2463/121* (2013.01); ***H04L 63/0807*** (2013.01)

(57) **ABSTRACT**

A forwarding method is applied to a constrained node and includes: receiving authentication information; determining whether the authentication information is received for the first time; and if the authentication information is received not for the first time, forwarding the authentication information; or if the authentication information is received for the first time, determining whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discarding the authentication information, or if the authentication information is valid authentication information, verifying the valid authentication information, and forwarding the valid authentication information after the verification succeeds.



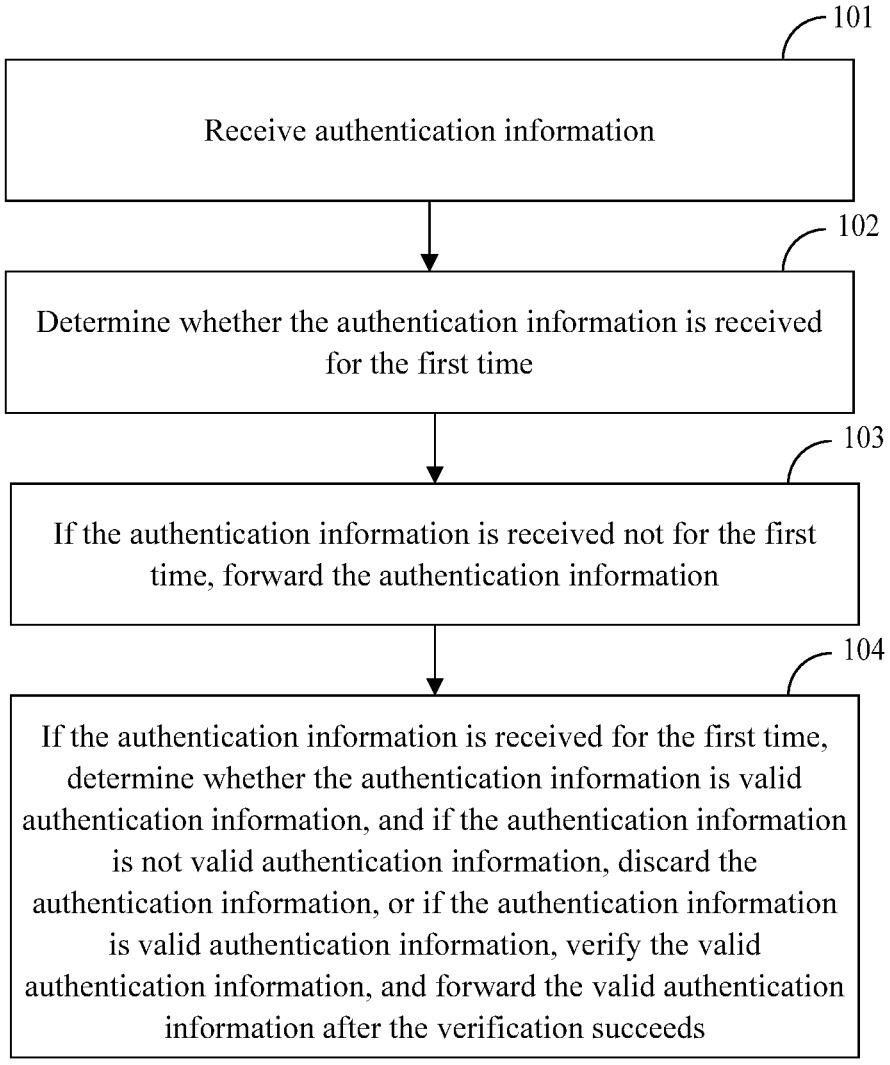

101
Receive authentication information
102
Determine whether the authentication information is received for the first time
103
If the authentication information is received not for the first time, forward the authentication information
104
If the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds

FIG. 1

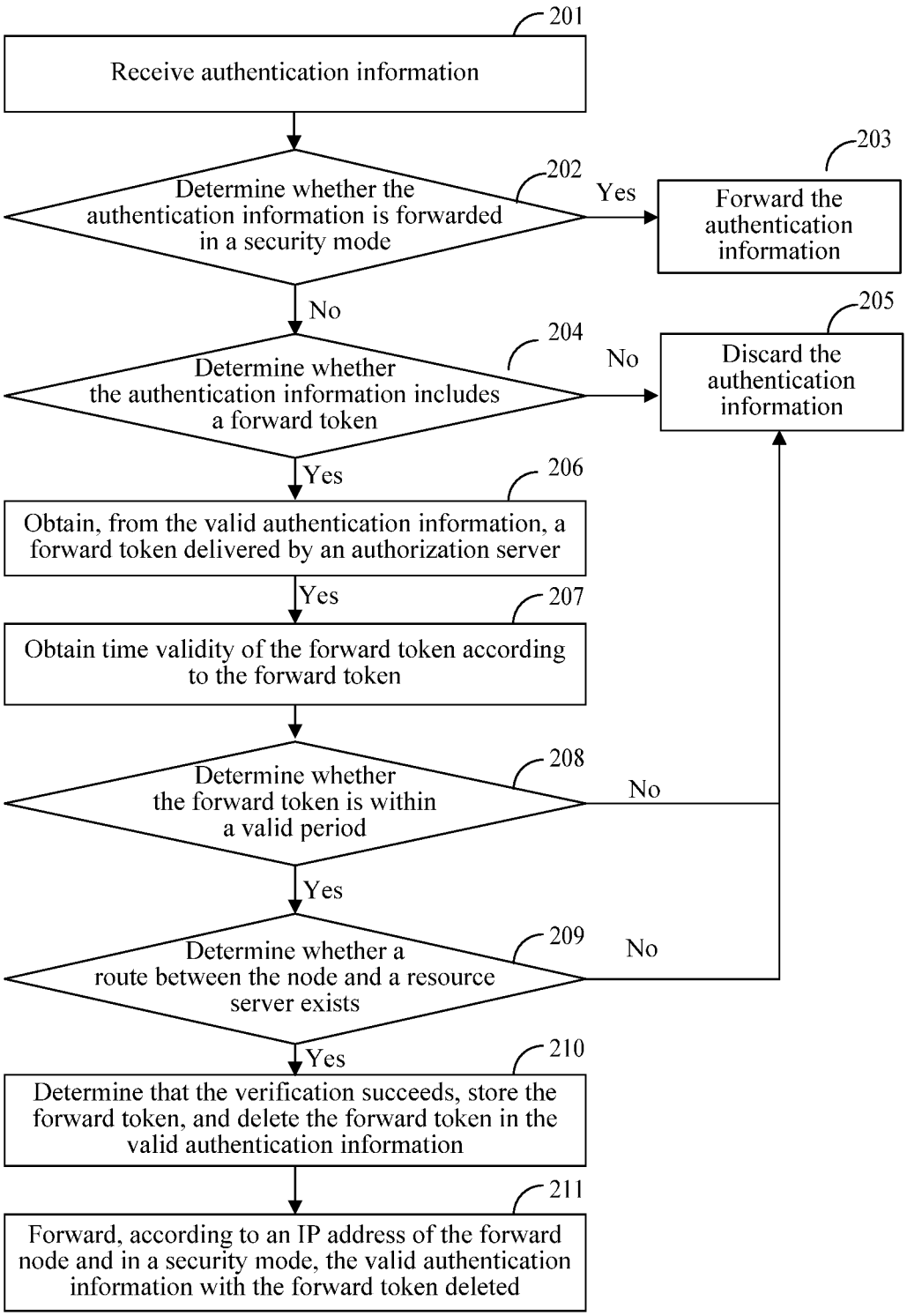

201
Receive authentication information
202
Determine whether the authentication information is forwarded in a security mode
Yes
203
Forward the authentication information
No
204
Determine whether the authentication information includes a forward token
No
205
Discard the authentication information
Yes
206
Obtain, from the valid authentication information, a forward token delivered by an authorization server
Yes
207
Obtain time validity of the forward token according to the forward token
208
Determine whether the forward token is within a valid period
No
Yes
209
Determine whether a route between the node and a resource server exists
No
Yes
210
Determine that the verification succeeds, store the forward token, and delete the forward token in the valid authentication information
211
Forward, according to an IP address of the forward node and in a security mode, the valid authentication information with the forward token deleted

FIG. 2

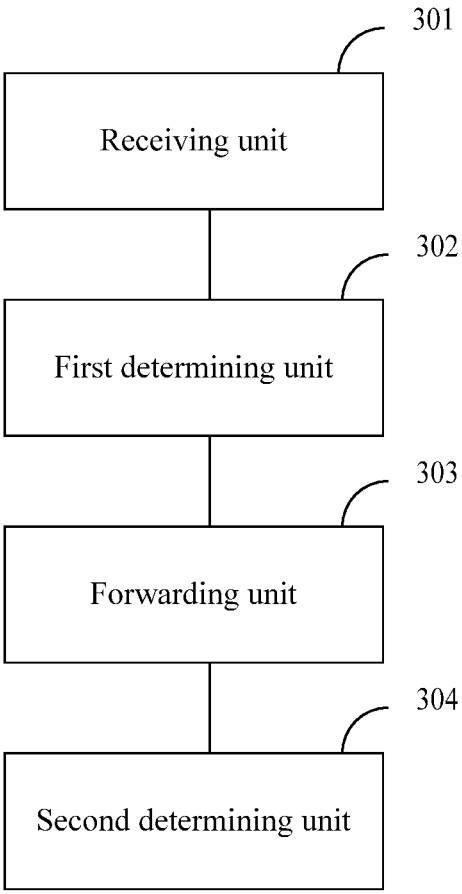

301
Receiving unit
302
First determining unit
303
Forwarding unit
304
Second determining unit

FIG. 3

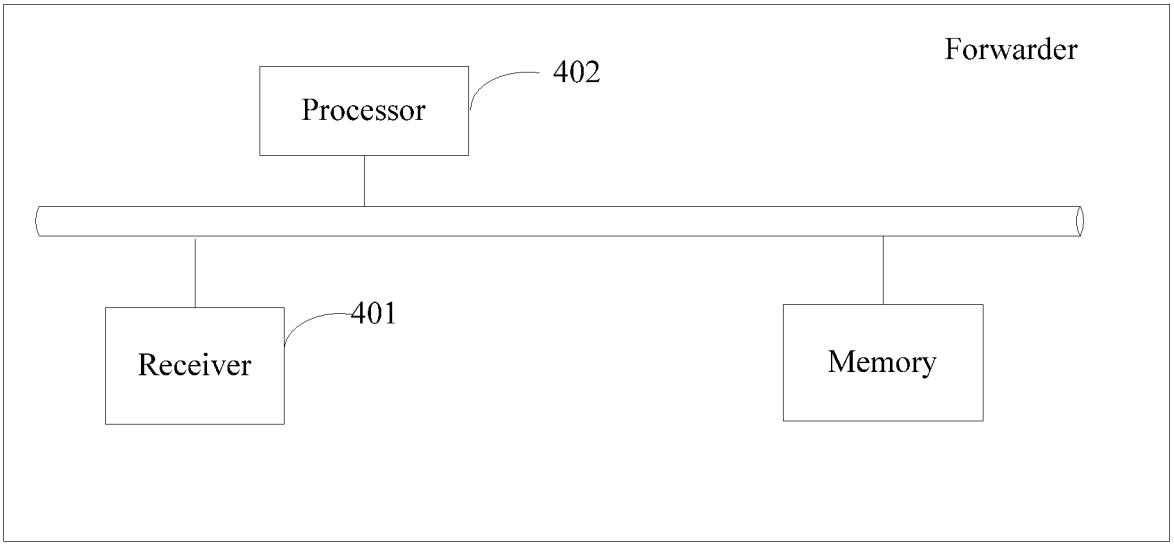


FIG. 4

FORWARDING METHOD, FORWARDING APPARATUS, AND FORWARDER FOR AUTHENTICATION INFORMATION IN INTERNET OF THINGS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 15/639,248, filed on Jun. 30, 2017, which is a continuation of International Patent Application No. PCT/CN2015/096300, filed on Dec. 3, 2015, which claims priority to Chinese Patent Application No. 201510003726.5, filed on Jan. 4, 2015. All of the aforementioned applications are hereby incorporated by reference in their entireties.

TECHNICAL FIELD

[0002] The present application relates to the field of the Internet of Things, and in particular, to a forwarding method, a forwarding apparatus, and a forwarder for authentication information in the Internet of Things.

BACKGROUND

[0003] The Internet of Things brings great convenience to people's life. In some approaches, authorization and authentication methods used by the Internet of Things both use a push model as a basic framework. For example, when a client requests a resource from a resource server (RS) on the other side of the Internet of Things or performs a resource operation, the client first needs to send a resource obtaining request to the RS, and after the RS returns information about an authorization server (AS), the client requests authorization from the AS. After obtaining an authorization credential from the AS, the client requests authentication from the RS by using the Datagram Transport Layer Security (DTLS) protocol. After authentication by the RS on the client succeeds, the client may request the resource from the RS or perform the resource operation.

[0004] The client may be unable to communicate with the RS directly. In this case, authentication information sent by the client to the RS needs to be forwarded by another node. However, if the node that forwards an authentication request is a constrained node, because a constrained node has a limited quantity of resources, in particular, when bandwidth resources and power supply resources are limited, quality of communication between the client and the RS is affected directly.

[0005] All nodes, including constrained nodes, in the Internet of Things forward authentication information unconditionally without filtering the information. If in an actual situation, a client in the Internet of Things maliciously sends a large amount of authentication information to an RS on the other side of the Internet of Things, nodes located between the client and the RS need to forward a large quantity of malicious authentication messages unconditionally. If the nodes that forward the authentication information are constrained nodes, it may cause that a large quantity of bandwidth resources of these nodes are occupied, and that electric power is consumed quickly. As a result, overall performance of the Internet of Things is affected, and even the Internet of Things is paralyzed.

SUMMARY

[0006] Embodiments of the present application provide a forwarding method, a forwarding apparatus, and a forwarder for authentication information in the Internet of Things, so as to resolve a problem that in the Internet of Things, performance of the Internet of Things is affected because a constrained node forwards authentication information unconditionally.

[0007] To resolve the foregoing technical problem, the embodiments of the present application disclose the following technical solutions.

[0008] According to a first aspect, a forwarding method for authentication information in the Internet of Things is provided, where the method is applied to a constrained node and includes: receiving authentication information; determining whether the authentication information is received for the first time; and if the authentication information is received not for the first time, forwarding the authentication information; or if the authentication information is received for the first time, determining whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discarding the authentication information, or if the authentication information is valid authentication information, verifying the valid authentication information, and forwarding the valid authentication information after the verification succeeds.

[0009] With reference to the first aspect, in a first possible implementation manner of the first aspect, the determining whether the authentication information is received for the first time includes: if the authentication information is forwarded in a security mode, determining that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determining that the authentication information is received for the first time.

[0010] With reference to the first aspect, in a second possible implementation manner of the first aspect, the determining whether the authentication information is valid authentication information includes: if the authentication information includes a forward token, determining that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determining that the authentication information is not valid authentication information.

[0011] With reference to the first aspect, in a third possible implementation manner of the first aspect, the verifying the valid authentication information includes: obtaining, from the valid authentication information, a forward token delivered by an authorization server; determining whether the forward token is a legitimate token; and if the forward token is a legitimate token, determining that the verification succeeds; or if the forward token is not a legitimate token, determining that the verification fails.

[0012] With reference to the third possible implementation manner of the first aspect, in a fourth possible implementation manner of the first aspect, the determining whether the forward token is a legitimate token includes: obtaining time validity of the forward token according to the forward token; determining whether the forward token is within a valid period; if the forward token is within the valid period, determining whether a route between the node and the resource server exists; and if the route exists, determining that the forward token is a legitimate token.

[0013] With reference to the fourth possible implementation manner of the first aspect, in a fifth possible implementation manner of the first aspect, the forwarding the valid authentication information after the verification succeeds includes: obtaining a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtaining an IP address of each forwarding node, and forwarding the valid authentication information according to the IP address of the forwarding node.

[0014] With reference to the fifth possible implementation manner of the first aspect, in a sixth possible implementation manner of the first aspect, the forwarding the valid authentication information according to the IP address of the forwarding node includes: deleting the forward token in the valid authentication information; and forwarding, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0015] According to a second aspect, a forwarding apparatus for authentication information in the Internet of Things is provided, where the apparatus includes: a receiving unit configured to receive authentication information; a first determining unit configured to determine whether the authentication information is received for the first time; a forwarding unit configured to: if the authentication information is received not for the first time, forward the authentication information; and a second determining unit configured to: if the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds.

[0016] With reference to the second aspect, in a first possible implementation manner of the second aspect, the first determining unit is configured to: if the authentication information is forwarded in a security mode, determine that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determine that the authentication information is received for the first time.

[0017] With reference to the second aspect, in a second possible implementation manner of the second aspect, the second determining unit is configured to: if the authentication information includes a forward token, determine that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determine that the authentication information is not valid authentication information.

[0018] With reference to the second aspect, in a third possible implementation manner of the second aspect, the second determining unit includes a verification subunit, and the verification subunit is configured to: obtain, from the valid authentication information, a forward token delivered by an authorization server; determine whether the forward token is a legitimate token; and if the forward token is a legitimate token, determine that the verification succeeds; or if the forward token is not a legitimate token, determine that the verification fails.

[0019] With reference to the third possible implementation manner of the second aspect, in a fourth possible implementation manner of the second aspect, the verification subunit is further configured to: obtain time validity of the forward token according to the forward token; determine whether the forward token is within a valid period; if the forward token is within the valid period, determine whether a route between the node and the resource server exists; and if the route exists, determine that the forward token is a legitimate token.

[0020] With reference to the fourth possible implementation manner of the second aspect, in a fifth possible implementation manner of the second aspect, the forwarding the valid authentication information after the verification succeeds includes: the second determining unit further includes a valid authentication information forwarding subunit, and the valid authentication information forwarding subunit is configured to: obtain a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtain an IP address of each forwarding node, and forward the valid authentication information according to the IP address of the forwarding node.

[0021] With reference to the fifth possible implementation manner of the second aspect, in a sixth possible implementation manner of the second aspect, the valid authentication information forwarding subunit is further configured to: delete the forward token in the valid authentication information; and forward, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0022] According to a third aspect, a forwarder for authentication information in the Internet of Things, where the forwarder includes: a receiver configured to receive authentication information; and a processor configured to determine whether the authentication information is received for the first time, where the processor is further configured to: if the authentication information is received not for the first time, forward the authentication information; and the processor is further configured to: if the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds.

[0023] With reference to the third aspect, in a first possible implementation manner of the third aspect, the processor is configured to: if the authentication information is forwarded in a security mode, determine that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determine that the authentication information is received for the first time.

[0024] With reference to the third aspect, in a second possible implementation manner of the third aspect, the processor is configured to: if the authentication information includes a forward token, determine that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determine that the authentication information is not valid authentication information.

[0025] With reference to the third aspect, in a third possible implementation manner of the third aspect, the pro-

cessor is configured to: obtain, from the valid authentication information, a forward token delivered by an authorization server; determine whether the forward token is a legitimate token; and if the forward token is a legitimate token, determine that the verification succeeds; or if the forward token is not a legitimate token, determine that the verification fails.

[0026] With reference to the third possible implementation manner of the third aspect, in a fourth possible implementation manner of the third aspect, the processor is configured to: obtain time validity of the forward token according to the forward token; determine whether the forward token is within a valid period; if the forward token is within the valid period, determine whether a route between the node and the resource server exists; and if the route exists, determine that the forward token is a legitimate token.

[0027] With reference to the fourth possible implementation manner of the third aspect, in a fifth possible implementation manner of the third aspect, the processor is configured to: obtain a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtain an IP address of each forwarding node, and forward the valid authentication information according to the IP address of the forwarding node.

[0028] With reference to the fifth possible implementation manner of the third aspect, in a sixth possible implementation manner of the third aspect, the processor is further configured to: delete the forward token in the valid authentication information; and forward, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0029] The embodiments of the present application disclose a forwarding method for authentication information in the Internet of Things. In the method, after receiving authentication information for the first time, a constrained node verifies the authentication information, and forwards the authentication information after the verification succeeds. This prevents a large amount of malicious authentication information from occupying bandwidth and consuming electric power of the constrained node that forwards the authentication information. In another case, when the authentication information is received not for the first time, the constrained node directly forwards the authentication information, so as to avoid wasting of system resources and improve performance of the Internet of Things.

BRIEF DESCRIPTION OF DRAWINGS

[0030] To describe the technical solutions in the embodiments of the present application more clearly, the following briefly describes the accompanying drawings required for describing the embodiments. The accompanying drawings in the following description show merely some embodiments of the present application, and a person of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0031] FIG. **1** shows a flowchart of a forwarding method for authentication information in the Internet of Things according to an embodiment of the present application;

[0032] FIG. **2** shows a flowchart of a forwarding method for authentication information in the Internet of Things according to an embodiment of the present application;

[0033] FIG. **3** shows a schematic diagram of a forwarding apparatus for authentication information in the Internet of Things according to an embodiment of the present application; and

[0034] FIG. **4** shows a schematic diagram of a forwarder for authentication information in the Internet of Things according to an embodiment of the present application.

DESCRIPTION OF EMBODIMENTS

[0035] The following embodiments of the present application provide a forwarding method, a forwarding apparatus, and a forwarder for authentication information in the Internet of Things, so as to improve performance of the Internet of Things.

[0036] The following clearly describes the technical solutions in the embodiments of the present application with reference to the accompanying drawings in the embodiments of the present application. The described embodiments are merely a part rather than all of the embodiments of the present application. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present application without creative efforts shall fall within the protection scope of the present application.

[0037] In the embodiments of the present application, a constrained node refers to a node with limited capabilities in computing, storage, and power supply and limited bandwidth, especially a node with a limited power supply capability and limited bandwidth, for example, a mobile terminal such as a mobile phone that may act as a node in the Internet of Things. A "constrained node" in the embodiments of the present application may alternatively be a constrained node or a constrained device specified in RFC 7228 of the Internet Engineering Task Force (IETF).

[0038] As shown in FIG. **1**, an embodiment of the present application provides a flowchart of a forwarding method for authentication information in the Internet of Things. As shown in FIG. **1**, the method is applied to a constrained node.

[0039] The method includes the following steps.

[0040] **S101**: Receive authentication information.

[0041] **S102**: Determine whether the authentication information is received for the first time.

[0042] That the authentication information is received for the first time means that the node receives, for the first time, the current authentication information sent by a source client to a destination resource server.

[0043] In **S102**, the determining whether the authentication information is received for the first time includes: if the authentication information is forwarded in a security mode, determining that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determining that the authentication information is received for the first time.

[0044] **S103**: If the authentication information is received not for the first time, forward the authentication information.

[0045] The determining whether the authentication information is valid authentication information includes: if the authentication information includes a forward token, determining that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determining that the authentication information is not valid authentication information.

[0046] S**104**: If the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds.

[0047] In S**104**, the determining whether the authentication information is valid authentication information includes: if the authentication information includes a forward token, determining that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determining that the authentication information is not valid authentication information.

[0048] The authentication information may be the first handshake message (Client Hello).

[0049] In this embodiment of the present application, authentication information that is received for the first time and is not valid may be considered to be malicious authentication information. Discarding the malicious authentication information may avoid wasting of resources of the constrained node.

[0050] In this embodiment of the present application, a client obtains authorization from an authorization server, and the authorization server delivers a forward token while delivering an authorization token. The forward token may carry information such as time validity of the forward token, an IP address of the client, an address of the resource server, and a signature of the authorization server.

[0051] In the forwarding method for authentication information in the Internet of Things according to this embodiment of the present application, after receiving authentication information for the first time, a constrained node first determines whether the authentication information is valid authentication information. If the authentication information is valid authentication information, the constrained node verifies the valid authentication information, and forwards the valid authentication information after the verification succeeds. This prevents a large amount of malicious authentication information from occupying bandwidth and consuming electric power of the constrained node that forwards the authentication information. In another case, when the authentication information is received not for the first time, the constrained node directly forwards the authentication information, so as to avoid wasting of system resources and improve performance of the Internet of Things.

[0052] Actually, the method in this embodiment of the present application may be applied to a constrained node. When a client sending authentication information comes from a different domain, the method in this embodiment may be applied to a proxy server as well. In this case, the proxy server may also be considered as a constrained node.

[0053] In S**104**, the verifying the valid authentication information includes: obtaining, from the authentication information, a forward token delivered by an authorization server; determining whether the forward token is a legitimate token; and if the forward token is a legitimate token, determining that the verification succeeds; or if the forward token is not a legitimate token, determining that the verification fails.

[0054] The forward token carried in the authentication information may replace a data field in the first handshake message with a forward token.

[0055] The determining whether the forward token is a legitimate token includes: obtaining time validity of the forward token according to the forward token; determining whether the forward token is within a valid period; if the forward token is within the valid period, determining whether a route between the node and the resource server exists; and if the route exists, determining that the forward token is a legitimate token.

[0056] The forwarding the authentication information after the verification succeeds includes: obtaining a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtaining an Internet Protocol IP address of each forwarding node, and forwarding the authentication information according to the IP address of the forwarding node.

[0057] There may be multiple routes between the client and the resource server. Forwarding the valid authentication information in all routes can avoid a failure in delivering the valid authentication information to the resource server in time in the case of a single route due to a line failure, line interference, a relatively long delay, or the like.

[0058] The forwarding the authentication information according to the IP address of the forwarding node includes: deleting the forward token in the valid authentication information; and forwarding, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0059] The forward token in the valid authentication information is deleted, and the valid authentication information is forwarded in a security mode. Therefore, after receiving the authentication information, a next node may determine without further verification that the authentication information is received not for the first time. This reduces resources of the constrained node and shortens a time for the authentication information to travel from the client to the resource server. The valid authentication information with the forward token deleted still contains all subsequent information that is of the authentication information and that is from the source address to the destination address.

[0060] In the forwarding method for authentication information in the Internet of Things according to this embodiment of the present application, after receiving authentication information for the first time, a constrained node determines whether the authentication information is valid authentication information, and if the authentication information is valid authentication information, the constrained node verifies the valid authentication information, and forwards the valid authentication information after the verification succeeds. This prevents a large amount of malicious authentication information from occupying bandwidth and consuming electric power of the constrained node that forwards the authentication information. In another case, when the authentication information is received not for the first time, the constrained node directly forwards the authentication information, so as to avoid wasting of system resources and improve performance of the Internet of Things.

[0061] FIG. **2** shows a flowchart of a forwarding method for authentication information in the Internet of Things according to an embodiment of the present application. The

method is applied to a constrained node. As shown in FIG. **2**, the method includes the following steps.

[0062] S**201**: Receive authentication information.

[0063] S**202**: Determine whether the authentication information is forwarded in a security mode, where if the authentication information is forwarded in a security mode, that is, the authentication information is received not for the first time, S**203** continues; or if the authentication information is forwarded not in a security mode, that is, the authentication information is received for the first time, S**204** continues.

[0064] S**203**: Forward the authentication information.

[0065] S**204**: Determine whether the authentication information includes a forward token; and if the authentication information does not include a forward token, that is, the authentication information is not valid authentication information, perform S**205**, or if the authentication information includes a forward token, that is, the authentication information is valid authentication information, perform S**206**.

[0066] S**205**: Discard the authentication information.

[0067] S**206**: Obtain, from the valid authentication information, the forward token delivered by an authorization server.

[0068] S**207**: Obtain time validity of the forward token according to the forward token.

[0069] S**208**: Determine whether the forward token is within a valid period; and if the forward token is not within the valid period, perform S**205**, or if the forward token is within the valid period, perform S**209**.

[0070] S**209**: Determine whether a route between the node and a resource server exists; and if the route does not exist, perform S**205**, or if the route exists, perform S**210**.

[0071] S**210**: Determine that the verification succeeds, store the forward token, and delete the forward token in the valid authentication information.

[0072] S**211**: Forward, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0073] In the forwarding method for authentication information in the Internet of Things according to this embodiment of the present application, after receiving authentication information for the first time, a constrained node verifies the authentication information, and forwards the authentication information after the verification succeeds. This prevents a large amount of malicious authentication information from occupying bandwidth and consuming electric power of the constrained node that forwards the authentication information. In another case, when the authentication information is received not for the first time, the constrained node directly forwards the authentication information, so as to avoid wasting of system resources and improve performance of the Internet of Things.

[0074] Corresponding to the foregoing methods, an embodiment of the present application further provides a forwarding apparatus for authentication information in the Internet of Things. FIG. **3** shows a schematic diagram of a structure of a forwarding apparatus for authentication information in the Internet of Things according to an embodiment of the present application. As shown in FIG. **3**, the apparatus includes: a receiving unit **301** configured to receive authentication information; a first determining unit **302** configured to determine whether the authentication information is received for the first time; a forwarding unit **303** configured to: if the authentication information is received not for the first time, forward the authentication information; and a second determining unit **304** configured to: if the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds.

[0075] Optionally, the first determining unit **302** is configured to: if the authentication information is forwarded in a security mode, determine that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determine that the authentication information is received for the first time.

[0076] Optionally, the second determining unit **304** is configured to: if the authentication information includes a forward token, determine that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determine that the authentication information is not valid authentication information.

[0077] Optionally, the second determining unit **304** includes a verification subunit, and the verification subunit is configured to: obtain, from the valid authentication information, a forward token delivered by an authorization server; determine whether the forward token is a legitimate token; and if the forward token is a legitimate token, determine that the verification succeeds; or if the forward token is not a legitimate token, determine that the verification fails.

[0078] Optionally, the verification subunit is further configured to: obtain time validity of the forward token according to the forward token; determine whether the forward token is within a valid period; if the forward token is within the valid period, determine whether a route between the node and a resource server exists; and if the route exists, determine that the forward token is a legitimate token.

[0079] Optionally, the second determining unit **304** further includes a valid authentication information forwarding subunit, and the valid authentication information forwarding subunit is configured to: obtain a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtain an IP address of each forwarding node, and forward the valid authentication information according to the IP address of the forwarding node.

[0080] Optionally, the valid authentication information forwarding subunit is further configured to: delete the forward token in the valid authentication information; and forward, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0081] With the forwarding apparatus for authentication information in the Internet of Things according to this embodiment of the present application, a large amount of malicious authentication information is prevented from occupying bandwidth and consuming electric power of a constrained node that forwards authentication information, and performance of the Internet of Things is improved.

[0082] FIG. **4** shows a schematic diagram of a forwarder for authentication information in the Internet of Things

according to an embodiment of the present application. As shown in FIG. **4**, the forwarder includes: a receiver **401** configured to receive authentication information; and a processor **402** configured to determine whether the authentication information is received for the first time, where the processor **402** is further configured to: if the authentication information is received not for the first time, forward the authentication information; and the processor **402** is further configured to: if the authentication information is received for the first time, determine whether the authentication information is valid authentication information, and if the authentication information is not valid authentication information, discard the authentication information, or if the authentication information is valid authentication information, verify the valid authentication information, and forward the valid authentication information after the verification succeeds.

[0083] Optionally, the processor **402** is configured to: if the authentication information is forwarded in a security mode, determine that the authentication information is received not for the first time; or if the authentication information is forwarded not in a security mode, determine that the authentication information is received for the first time.

[0084] Optionally, the processor **402** is configured to: if the authentication information includes a forward token, determine that the authentication information is valid authentication information; or if the authentication information does not include a forward token, determine that the authentication information is not valid authentication information.

[0085] Optionally, the processor **402** is configured to: obtain, from the valid authentication information, a forward token delivered by an authorization server; determine whether the forward token is a legitimate token; and if the forward token is a legitimate token, determine that the verification succeeds; or if the forward token is not a legitimate token, determine that the verification fails.

[0086] Optionally, the processor **402** is configured to: obtain time validity of the forward token according to the forward token; determine whether the forward token is within a valid period; if the forward token is within the valid period, determine whether a route between the node and a resource server exists; and if the route exists, determine that the forward token is a legitimate token.

[0087] Optionally, the processor **402** is configured to: obtain a forwarding node in each existing route, where the forwarding node is a node that receives the valid authentication information forwarded by the node; and obtain an IP address of each forwarding node, and forward the valid authentication information according to the IP address of the forwarding node.

[0088] Optionally, the processor **402** is further configured to: delete the forward token in the valid authentication information; and forward, according to the IP address of the forwarding node and in a security mode, the valid authentication information with the forward token deleted.

[0089] The forwarder for authentication information in the Internet of Things according to this embodiment of the present application, after authentication information is received for the first time, determines whether the authentication information is valid authentication information, verifies the valid authentication information, and forwards the authentication information after the verification succeeds. This prevents not-valid authentication information from occupying bandwidth and consuming electric power of a constrained node, and improves performance of the Internet of Things.

[0090] The embodiments of the present application disclose a forwarding method, a forwarding apparatus, and a forwarder for authentication information in the Internet of Things. In the embodiments of the present application, after receiving authentication information for the first time, a constrained node determines whether the authentication information is valid authentication information, verifies the valid authentication information, and forwards the authentication information after the verification succeeds. This prevents invalid authentication information, for example, a large amount of malicious authentication information, from occupying bandwidth and consuming electric power of the constrained node that forwards the authentication information. In another case, when the authentication information is received not for the first time, the constrained node directly forwards the authentication information, so as to avoid wasting of system resources and improve performance of the Internet of Things.

[0091] It may be clearly understood by a person skilled in the art that the technology in the embodiments of the present application may be implemented by software plus necessary general-purpose hardware. The general-purpose hardware includes a general-purpose integrated circuit, a general-purpose CPU, a general-purpose memory, a general-purpose component, and the like. Certainly, the technology may be implemented as well by application-specific hardware, including an application-specific integrated circuit, an application-specific CPU, an application-specific memory, an application-specific component, and the like. However, in many cases, the former one is more preferred. Based on such an understanding, the technical solutions may be implemented in a form of a software product. The software product is stored in a storage medium, such as a read-only memory (ROM), a random-access memory (RAM), a hard disk, or an optical disc, and includes a quantity of instructions for instructing a computer device (which may be a personal computer, a server, or a network device) to perform the methods described in the embodiments or some parts of the embodiments of the present application.

[0092] The embodiments in this specification are all described in a progressive manner. For same or similar parts in the embodiments, mutual reference may be made. Each embodiment focuses on what is different from other embodiments. Especially, a system embodiment is essentially similar to a method embodiment, and therefore is described briefly. For related information, reference may be made to descriptions about this in the method embodiment.

[0093] The foregoing descriptions are implementation manners of the present application, and are not intended to limit the protection scope of the present application. Any modification, equivalent replacement, and improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.

What is claimed is:

1. A method implemented by a constrained node and comprising:

receiving, from an Internet of things (IoT) client, authentication information a first time;

performing, in response to receiving the authentication information the first time, a first verification of the authentication information;

receiving the authentication information a second time; and

forwarding, in response to receiving the authentication information the second time, the authentication information without performing a second verification of the authentication information.

2. The method of claim **1**, further comprising determining that the authentication information is received for the first time when receiving the authentication information in a non-security mode.

3. The method of claim **1**, further comprising further forwarding the authentication information when the first verification succeeds.

4. The method of claim **3**, further comprising discarding the authentication information when the first authentication fails.

5. The method of claim **3**, wherein the authentication information comprises a forward token.

6. The method of claim **5**, wherein the first verification is successful when the forward token is a legitimate token.

7. The method of claim **6**, wherein the forward token is the legitimate token when time validity of the forward token is within a valid period and a route between the constrained node and a resource server exists.

8. The method of claim **5**, further comprising:

deleting the forward token from the authentication information to obtain modified authentication information; and

further forwarding the modified authentication information in a security mode.

9. A constrained node comprising:

a receiver configured to:

receive, from an Internet of things (IoT) client, authentication information a first time, and

receive the authentication information a second time; and

a processor coupled to the receiver and configured to:

perform, in response to receiving the authentication information the first time, a first verification of the authentication information, and

forward, in response to receiving the authentication information the second time, the authentication information without performing a second verification of the authentication information.

10. The constrained node of claim **9**, wherein the processor is further configured to determine that the authentication information is received for the first time when receiving the authentication information in a non-security mode.

11. The constrained node of claim **9**, wherein the processor is further configured to further forward the authentication information when the first verification succeeds.

12. The constrained node of claim **11**, wherein the processor is further configured to discard the authentication information when the first authentication fails.

13. The constrained node of claim **11**, wherein the authentication information comprises a forward token.

14. The constrained node of claim **13**, wherein the first verification is successful when the forward token is a legitimate token.

15. The constrained node of claim **14**, wherein the forward token is the legitimate token when time validity of the forward token is within a valid period and a route between the constrained node and a resource server exists.

16. The constrained node of claim **13**, where the processor is further configured to delete the forward token from the authentication information to obtain modified authentication information, and wherein the receiver is further configured to further forward the modified authentication information in a security mode.

17. A computer program product comprising instructions for storage on a non-transitory medium and that, when executed by a processor, cause a constrained node to:

receive, from an Internet of things (IoT) client, authentication information a first time;

perform, in response to receiving the authentication information the first time, a first verification of the authentication information;

receive the authentication information a second time; and

forward, in response to receiving the authentication information the second time, the authentication information without performing a second verification of the authentication information.

18. The computer program product of claim **17**, wherein the instructions further cause the constrained node to determine that the authentication information is received for the first time when receiving the authentication information in a non-security mode.

19. The computer program product of claim **17**, wherein the instructions further cause the constrained node to further forward the authentication information when the first verification succeeds.

20. The computer program product of claim **19**, wherein the instructions further cause the constrained node to discard the authentication information when the first authentication fails.

* * * * *