NETWORK DISTRIBUTION METHOD AND APPARATUS FOR DUAL-MODE INTERNET-OF-THINGS DEVICE, AND STORAGE MEDIUM

CROSS REFERENCE TO RELATED APPLICATIONS

This application is based on and claims priority to Chinese patent application No. 202210386928.2, filed on April 13, 2022, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

The present disclosure relates to a field of network configuration technologies of an internet of things (IoT) device, in particular to a method and apparatus for configuring a network for a dual-mode IoT device, and a storage medium.

BACKGROUND

Currently, there are two main methods for configuring a network for an IoT device, namely, SmartConfig method and wireless access point (AP) method.

A basic principle of the SmartConfig method is provided as follows.

The IoT device enters a wireless fidelity (Wi-Fi) promiscuous mode to monitor and capture surrounding Wi-Fi messages. Since the IoT device is not networked, and all the fields in a captured message are encrypted except for an 802.11 media access control (MAC) header. The IoT device cannot obtain contents of original data (e.g., payload), but it can obtain feature data of a message. Although an entire data part of the message is encrypted, a length of the message, sent MAC and target MAC can be learned. That is, a cell phone application (APP) encodes a service set identifier (SSID) and a character string of a password of a router by using length variation according to an agreement, and sends them via a broadcast packet or multicast packet of a user datagram protocol (UDP). After capturing a UDP message, the IoT device decodes the UDP message according to the agreement, to obtain the SSID and a password of a target Wi-Fi router perform active networking.

A basic principle of a wireless AP network configuration method is provided as follows.

An APP terminal connects to a target router, obtains the SSID of the target router and a manually entered password, and triggers a Wi-Fi module to enter an AP network configuration

mode. The APP terminal requests to connect to an AP hotspot issued by the Wi-Fi module and sends the SSID and the password of the target router to the Wi-Fi module. The Wi-Fi module may be networked after receives the SSID and the password of the router.

The existing SmartConfig network configuration method is often limited to a certain type of Wi-Fi module, and has a long operation duration and low success rate, which are not conducive to a popularization of network configuration for the IoT device. The existing SmartConfig network configuration method is often customized for specific Wi-Fi chips of manufacturers, some manufacturers support length variation encoding, some manufacturers support multicast address variation encoding, so that encoding modes of different chip manufacturers are different. It is complex that the APP terminal is compatible with the SmartConfig network configuration methods of various manufacturers. Therefore, APP terminals applicable to SmartConfig network configuration methods do not have universality.

For the wireless AP network configuration method, although the success rate is improved, many existing Wi-Fi modules do not support its operating mode, and network configuration process is complicated and user experience is poor.

Therefore, how to improve the success rate and universality of the network configuration for IoT device while simplifying the process has become an urgent problem to be solved in this field.

SUMMARY

The embodiments of the present disclosure provides a method for configuring a network for a dual-mode IoT device, an apparatus for configuring a network for a dual-mode IoT device and a storage medium, to solve the problem that the existing IoT device network configuration methods are executed through complex network configuration processes and have a low success rate and/or universality.

The technical solutions of the embodiments of the present disclosure are realized in the following ways.

According to a first aspect of embodiments of the present disclosure, a method for configuring a network for a dual-mode IoT device, applied to an APP terminal, is provided. The method includes:

establishing a bluetooth low energy (BLE) connection with a target IoT device;

after establishing the BLE connection, sending a session key request message to the target

IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, in which a data structure of the communication data protocol includes: an operation code, a function point identifier (ID), and function point data;

after receiving a session key returned by the target IoT device, generating encrypted network configuration information based on the session key; and

sending the encrypted network configuration information to the target IoT device, so that the target IoT device performs network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above method, generating the encrypted network configuration information based on the session key, includes:

sending a request for network configuration binding token information to a server; and

after receiving the network configuration binding token information fed back by the server, encrypting the network configuration binding token information, a pre-determined SSID and a connection password of a router according to the session key, to generate the encrypted network configuration information.

In some embodiments, based on the above method, after sending the encrypted network configuration information to the target IoT device, the method further includes:

after determining that the target IoT device receives the encrypted network configuration information, querying a server on whether the network configuration binding is successful by polling; and

in response to receiving network configuration binding success information fed back by the server, displaying first information indicating that the network configuration binding is successful.

In some embodiments, based on the above method, establishing the BLE connection with the target IoT device includes:

searching for a BLE broadcast frame, in which the BLE broadcast frame carries a device ID, a MAC, and an APP ID;

in response to detecting the BLE broadcast frame, determining whether the BLE broadcast frame matches the APP terminal according to the APP ID;

in response to determining that the BLE broadcast frame matches the APP terminal, querying the server on detailed information of a corresponding device according to the device ID, in which the detailed information at least includes an initialization key;

after obtaining the detailed information, displaying a list of alternative devices; and

determining an IoT device in the list of alternative devices as the target IoT device according to a selection input of a user, and establishing the BLE connection.

In some embodiments, based on the above method, the method further includes:

in response to determining that the BLE broadcast frame does not match the APP terminal according to the APP ID or in response to not obtaining the detailed information, discarding the BLE broadcast frame; and

in response to determining that the list of alternative devices is not displayed within a first preset duration, displaying second information indicating a search failure.

In some embodiments, based on the above method, before searching for the BLE broadcast frame, the method further includes:

determining an SSID and a connection password of a router to be connected according to a user input.

In some embodiments, based on the above method, after sending the session key request message to the target IoT device in one or more packets according to the communication data protocol and the packetizing protocol, the method further includes:

in response to receiving initialization key verification failure information returned by the target IoT device, displaying third information indicating a network configuration failure.

In some embodiments, based on the above method, after querying the server on whether the network configuration binding is successful by polling, the method further includes:

in response to not obtaining result information related to the target IoT device by polling within a second preset duration, displaying fourth information indicating a network configuration binding failure.

According to a second aspect of embodiments of the present disclosure, a method for configuring a network for a dual-mode IoT device, applied to an IoT device, is provided. The method includes:

establishing a BLE connection with an APP terminal;

after establishing the BLE connection, receiving a session key request message sent by in one or more packets the APP terminal according to a preset communication data protocol and a packetizing protocol;

assembling the session key request message according to the packetizing protocol, and

splitting an assembled message according to the communication data protocol to obtain an initialization key of the IoT device;

verifying the initialization key, and feeding back a session key in response to a successful verification; and

after receiving encrypted network configuration information that is encrypted according to the session key and sent by the APP terminal, performing network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above method, performing the network configuration binding according to the encrypted network configuration information, includes:

decrypting the encrypted network configuration information according to the session key, to obtain network configuration binding token information, a SSID and a connection password of a router, and sending a reception success signal to the APP terminal;

sending a networking request to the corresponding router according to the SSID and the connection password of the router; and

after successful networking, sending a registration or login request to a server according to the network configuration binding token information.

In some embodiments, based on the above method, before establishing the BLE connection with the APP terminal, the method further includes:

after entering a network configuration state, sending a BLE broadcast frame carrying a device ID, a MAC, and an APP ID according to a preset format.

According to a third aspect of embodiments of the present disclosure, a method for configuring a network for a dual-mode IoT device, applied to a server, is provided. The method includes:

after receiving a request for network configuration binding token information sent by an APP, sending the network configuration binding token information to the APP terminal;

in response to receiving a registration or login request sent by the IoT device after successful networking, performing a verification according to the network configuration binding token information carried in the registration or login request; and

performing a registration or login process of the IoT device in response to a successful verification, and binding the IoT device under a user name of the APP terminal.

In some embodiments, based on the above method, after performing the registration or login

process of the IoT device in response to the successful verification, and binding the IoT device under the user name of the APP terminal, the method further includes:

feeding back network configuration binding success information based on a polling request on whether network configuration binding is successful sent by the APP terminal.

According to a fourth aspect of embodiments of the present disclosure, an APP terminal is provided. The APP terminal includes:

a first processing module, configured to establish a BLE connection with a target IoT device;

a second processing module, configured to, after establishing the BLE connection, send a session key request message to the target IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, in which a data structure of the communication data protocol includes: an operation code, a function point ID, and function point data;

a third processing module, configured to, after receiving a session key returned by the target IoT device, generate encrypted network configuration information based on the session key; and

a fourth processing module, configured to send the encrypted network configuration information to the target IoT device, so that the target IoT device performs network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above APP, the third processing module includes:

a first processing sub-module, configured to send a request for network configuration binding token information to a server; and

a second processing sub-module, configured to, after receiving the network configuration binding token information fed back by the server, encrypt the network configuration binding token information, a pre-determined SSID and a connection password of a router according to the session key, to generate the encrypted network configuration information.

In some embodiments, the above APP terminal further includes:

a thirteenth processing module, configured to, after determining that the target IoT device receives the encrypted network configuration information, query a server on whether the network configuration binding is successful by polling; and

a fourteenth processing module, configured to, after receiving network configuration binding success information fed back by the server, display first information indicating that the network configuration binding is successful.

In some embodiments, based on the above APP, the first processing module includes:

a third processing sub-module, configured to search for a BLE broadcast frame, in which the BLE broadcast frame carries a device ID, a MAC, and an APP ID;

a fourth processing sub-module, configured to, in response to detecting a BLE broadcast frame, determine whether the BLE broadcast frame matches the APP terminal according to the APP ID;

a fifth processing sub-module, configured to, in response to determining that the BLE broadcast frame matches the APP terminal, query the server on detailed information of a corresponding device according to the device ID, in which the detailed information at least includes an initialization key;

a sixth processing sub-module, configured to, after obtaining the detailed information, display a list of alternative devices; and

a seventh processing sub-module, configured to determine an IoT device in the list of alternative devices as the target IoT device according to selection input of a user, and establish the BLE connection.

In some embodiments, the above APP terminal further includes:

a fifteenth processing module, configured to, in response to determining that the BLE broadcast frame does not match the APP terminal according to the APP ID or in response to not obtaining the detailed information, discard the BLE broadcast frame; and

a sixteenth processing module, configured to, in response to determining that the list of alternative devices is not displayed within a first preset duration, display second information indicating a search failure.

In some embodiments, before searching for the BLE broadcast frame, the above APP terminal further includes:

a seventeenth processing module, configured to determine a SSID and a connection password of a router to be connected according to user input.

In some embodiments, the above APP terminal further includes:

an eighteenth processing module, configured to, in response to receiving an initialization key verification failure information returned by the target IoT device, display third information indicating a network configuration failure.

In some embodiments, the above APP terminal further includes:

a nineteenth processing module, configured to, in response to not obtaining result information related to the target IoT device by polling within a second preset duration, display fourth information indicating a network configuration binding failure.

According to a fifth aspect of embodiments of the present disclosure, an IoT device is provided. The IoT device includes:

a fifth processing module, configured to establish a BLE connection with an APP terminal;

a sixth processing module, configured to, after establishing the BLE connection, receive a session key request message sent in one or more packets by the APP terminal according to a preset communication data protocol and a packetizing protocol;

a seventh processing module, configured to assemble the session key request message according to the packetizing protocol, and split the assembled message according to the communication data protocol, to obtain an initialization key of the IoT device;

an eighth processing module, configured to verify the initialization key, and feed back a session key in response to a successful verification; and

a ninth processing module, configured to, after receiving encrypted network configuration information that is encrypted according to the session key and sent by the APP terminal, perform network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above IoT device, the ninth processing module includes:

an eighth processing sub-module, configured to decrypt the encrypted network configuration information according to the session key, to obtain network configuration binding token information, a SSID and a connection password of a router, and send a reception success signal to the APP terminal;

a ninth processing sub-module, configured to send a networking request to the corresponding router according to the SSID and the connection password of the router; and

a tenth processing sub-module, configured to, after successful networking, send a registration or login request to a server according to the network configuration binding token information.

In some embodiments, the above IoT device further includes:

a twentieth processing module, configured to, after entering a network configuration state, send a BLE broadcast frame carrying a device ID, a MAC, and an APP ID according to a preset format.

According to a sixth aspect of embodiments of the present disclosure, a server is provided.

The server includes:

a tenth processing module, configured to, after receiving a request for network configuration binding token information sent by an APP terminal, send the network configuration binding token information to the APP terminal;

an eleventh processing module, configured to, in response to receiving a registration or login request sent by the IoT device after successful networking, perform a verification according to the network configuration binding token information carried in the registration or login request; and

a twelfth processing module, configured to perform a registration or login process of the IoT device in response to a successful verification, and bind the IoT device under a user name of the APP terminal.

In some embodiments, the above server further includes:

a twenty-first processing module, configured to feed back network configuration binding success information based on a polling request on whether network configuration binding is successful sent by the APP terminal.

According to a seventh aspect of embodiments of the present disclosure, a computer-readable storage medium having computer programs stored thereon is provided. When the computer programs are executed by a processor, the steps of the method for configuring a network for a dual-mode IoT device applied to an APP of the first aspect, or the steps of the method for configuring a network for a dual-mode IoT device applied to an IoT device of the second aspect, or the steps of the method for configuring a network for a dual-mode IoT device applied to a server of the third aspect are implemented.

Compared to the related art, the method for configuring a network for a dual-mode IoT device, the apparatus for configuring a network for a dual-mode IoT device and the storage medium provided by the embodiments of the present disclosure have at least the following beneficial effects.

In the embodiments of the present disclosure, the network configuration information is sent using the point-to-point connection via the BLE connection, rather than the broadcasting method, the multicasting method and other inefficient sending methods. Therefore, the method of the embodiments of the present disclosure has the advantages of high transmission efficiency, short configuration duration, and high network configuration success rate. Encryption based on a

currently acquired session key is conducive to improving the data security of network configuration. Data compilation based on the application-layer-based data communication protocol is no longer bound to the underlying capabilities of chips, which makes it effective for the chips of different manufacturers. Packetizing based on data type is no longer specific to corresponding functions of data, which makes the method of the present disclosure universally applicable.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a first schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an APP terminal provided by an embodiment of the present disclosure.

FIG. 2 is a second schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an APP terminal provided by an embodiment of the present disclosure.

FIG. 3 is a third schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an APP terminal provided by an embodiment of the present disclosure.

FIG. 4 is a fourth schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an APP terminal provided by an embodiment of the present disclosure.

FIG. 5 is a first schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an IoT device provided by an embodiment of the present disclosure.

FIG. 6 is a second schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an IoT device provided by an embodiment of the present disclosure.

FIG. 7 is a schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to a server provided by an embodiment of the present disclosure.

FIG. 8 is a schematic flowchart of an exemplary method for configuring a network for a dual-mode IoT device provided by an embodiment of the present disclosure.

FIG. 9 is a structural diagram of an APP terminal provided by an embodiment of the present disclosure.

FIG. 10 is a structural diagram of an IoT device provided by an embodiment of the present disclosure.

FIG. 11 is a structural diagram of a server provided by an embodiment of the present disclosure.

DETAILED DESCRIPTION

In order to make the technical problems to be solved, technical solutions and advantages of the present disclosure clearer, the following description is provided in detail in combination with the accompanying drawings and specific embodiments. In the following description, particular details such as specific configurations and components are provided only to aid in fully understanding the embodiments of the present disclosure. Those skilled in the art understood that various changes and modifications of the embodiments described herein can be made without departing from the scope and spirit of the present disclosure. For the sake of clarity and brevity, descriptions of well-known functions and structures are omitted from the following description.

It should be understood that references to “one embodiment” or “an embodiment” throughout the present disclosure imply that a particular feature, structure, or characteristic associated with the embodiment is included in at least one embodiment of the present disclosure. Therefore, “in one embodiment” or “in an embodiment” appearing at various places throughout the present disclosure may not necessarily refer to the same embodiment. Furthermore, these particular features, structures or characteristics may be combined in one or more embodiments in any suitable manner.

In the embodiments of the present disclosure, it should be understood that the magnitude of serial numbers of processes described below does not imply a sequential order of execution, and that the order of execution of the processes should be determined by their functions and inherent logics without constituting any limitation on implementation processes of the embodiments of the present disclosure.

It should be understood that the term “and/or” in this present disclosure is merely a description of association relations between associated objects, which indicates three relations. For example, A and/or B, may represent A exists alone, A and B both exist, and B exists alone. In addition, the character “/” in this present disclosure generally indicates that the associated objects before and after the character “/” is in an “or” relation.

In the embodiments of the present disclosure, it is understood that “B corresponding to A” means that B is associated with A, and B can be determined according to A. It should also be understood that although B can be determined according to A, it does not mean that B can only be determined according to A, B can also be determined according to A and/or other information.

The existing SmartConfig network configuring method is realized by UDP broadcasting or

multicasting. The SSID and the character string of the password are transmitted through length encoding, which is inefficient, takes a long operation duration, and has a low success rate. Moreover, the existing AP network configuring method relies on the specific operating mode of the Wi-Fi module and has complicated processes, it also requires the APP to jump to a setting page to connect to an AP hotspot of the IoT device, and then return to the APP terminal to send the SSID and the password of the router, which makes the processes complicated.

FIG. 1 is a schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an APP terminal provided by an embodiment of the present disclosure. The method includes the following steps.

At step S101, a BLE connection with a target IoT device is established.

At step S102, after establishing the BLE connection, a session key request message is sent to the target IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, in which a data structure of the communication data protocol includes an operation code, a function point ID, and function point data.

At step S103, after receiving a session key returned by the target IoT device, encrypted network configuration information is generated based on the session key.

At step S104, the encrypted network configuration information is sent to the target IoT device, so that the target IoT device performs network configuration binding according to the encrypted network configuration information.

In the embodiment of the present disclosure, when configures a network for the IoT device, the APP terminal first establishes the BLE connection with the target IoT device to be configured with a network, i.e., a point-to-point connection between the APP terminal and the target IoT device is established via the BLE connection first, which is a stable connection and has high data transmission efficiency, so as to facilitate accurate transmission of the subsequent data information and the like, and to further realize a short network configuration duration and a higher success rate. After establishing the BLE connection, the session key request message is generated based on a preset application-layer-based data communication protocol and sent to the target IoT device in one or more packets the message based on a preset packetizing protocol, so that the target IoT device can be informed of the request from the APP terminal after receiving the message and reply to the message. When a reply from the target IoT device is a session key, the encrypted network configuration information is generated based on the session key. The encrypted

network configuration information is sent to the target IoT device, so that the target IoT device may decrypt the encrypted network configuration information to obtain the network configuration information based on the session key, and further to perform network configuration binding.

In the embodiment of the present application, the network configuration binding refers to that the APP terminal configures the network for the target IoT device, and binds the target IoT device to a user name of the APP terminal after the target IoT device is networked.

It is understood that based on the BLE application-layer-based data communication protocol and the packetizing protocol, data transmission is performed with common rules, which make encapsulation and parsing simpler and makes the method more applicable.

In conclusion, in the embodiments of the present disclosure, the network configuration information is sent using the point-to-point connection via the BLE connection, rather than a broadcasting method, a multicasting method and other inefficient sending methods. Therefore, the method of the embodiments of the present disclosure has the advantages of high transmission efficiency, short configuration duration, and high network configuration success rate. Encryption based on a currently acquired session key is conducive to improving the data security of network configuration. Data compilation based on the application-layer-based data communication protocol is no longer bound to the underlying capabilities of chips, which makes it effective for the chips of different manufacturers. Packetizing based on data type is no longer specific to corresponding functions of data, which makes the method of the present disclosure universally applicable.

It should be noted that a data structure of the preset application-layer-based communication data protocol includes: an operation code, a function point ID, and function point data. An illustrative data structure can be referred to Table 1:

Table 1

operation code	function point ID	function point data	
		length	data field
1byte	2byte	2byte	nbyte

The operation code is configured to represent the function of data, for example, reading or writing data from the APP terminal to a device, responding to the success or failure of an operation of the APP terminal by the IoT device, and actively reporting to the APP terminal by the IoT device, which generally occupies 1 byte. The function point ID represents a specific function of the data, and can identify the function point of sending the SSID and the password of the router,

and the like, in the network configuration of the embodiments of the present disclosure, which generally occupies 2 bytes. The function point data represents sent specific parameter information, in which the length represents the number of bytes occupied by the data field, which generally occupies 2 bytes. The data field represents the specific parameters transmitted, such as, an initialization key, the SSID and the password of the router, and other information. Since a total length of the data frame sent by the BLE connection in a single transmission cannot exceed 20 bytes, when the length of the data field is greater than 15 bytes, the whole data information (including the operation code, the function point ID and the function point data) needs to be packetized according to the packetizing protocol, not only the function point data. The illustrative data structure after packetizing is shown in Table 2.

Table 2

Packet ID	Total number of packets	Packet index	Packet length	data
1byte	1byte	1byte	1byte	1-16byte

As shown in Table 2, the data structure after packetizing includes: a packet ID, a total number of packets, a packet index, a packet length and data. The packet ID occupies 1 byte, and when the data information is required to be packetized, the packet ID of each packet is the same. The total number of packets occupies 1 byte, which represents a serial number of the current packet in all the packets. The packet length occupies 1 byte, which represents that the length of the data in the current packet, in which the maximum length is 16 bytes, and preferably, all the packets are 16 bytes except a last packet. The data is the data in each packet.

It should also be noted that all information sent or received over the BLE connection in the embodiments of the present disclosure is required to be processed according to the application-layer-based communication data protocol and the packetizing protocol described above.

As illustrated in FIG. 2, in some embodiments, based on the above method, generating the encrypted network configuration information based on the session key includes the following steps.

At step S201, a request for network configuration binding token information is sent to a server.

At step S202, after receiving the network configuration binding token information fed back by the server, the network configuration binding token information, a pre-determined SSID and a connection password of a router according to the session key is encrypted, to generate the encrypted network configuration information.

In the embodiment of the present disclosure, when generating the encrypted network configuration information based on the session key, a request for network configuration binding token information is sent to the server first, to obtain the network configuration binding token information from the server. After the network configuration binding token information is received from the server, the network configuration binding token information, the pre-determined SSID and the connection password of the router are encrypted based on the session key, to obtain the encrypted network configuration information. The network configuration binding token information is configured to represent that the target IoT device is a legitimate device, and the SSID and the connection password of the router are used to enable the server to connect to the target IoT device.

In the embodiment of the present application, the network configuration binding token information refers to information configured for verifying and determining whether the target IoT device is a legitimate device in a network configuration binding process, and the network configuration binding token information includes user information.

As illustrated in FIG. 3, in some embodiments, based on the above method, after sending the encrypted network configuration information to the target IoT device, the method includes the following steps.

At step S301, after determining that the target IoT device receives the encrypted network configuration information, a server is queried on whether the network configuration binding is successful by polling.

At step S302, in response to receiving network configuration binding success information fed back by the server, first information indicating that the network configuration binding is successful is displayed.

In the embodiment of the present disclosure, after the encrypted network configuration information is sent to the target IoT device, in order to ensure that the target IoT device successfully receives the encrypted network configuration information, a feedback from the target IoT device is waited. Subsequent operations are performed after the feedback of the target IoT device is received. When it is determined that the target IoT device receives the encrypted network configuration information according to the feedback, it is determined that the target IoT device may perform network configuration with the server according to the encrypted network configuration information, and query the server on whether the network configuration is

successfully bound by polling, so as to learn a network configuration result in time. When the network configuration binding success information is received from the server, the first information indicating that the network configuration binding is successful is displayed, to inform the user that the target IoT device has been successfully configured a network, so as to improve the user experience.

As illustrated in FIG. 4, in some embodiments, based on the above method, establishing the BLE connection with the target IoT device includes the following steps.

At step S401, a BLE broadcast frame is searched, in which the BLE broadcast frame carries a device ID, a MAC, and an APP ID.

At step S402, in response to the BLE broadcast frame being detected, it is determined whether the BLE broadcast frame matches the APP terminal according to the APP ID.

At step S403, in response to determining that the BLE broadcast frame matches the APP terminal, the server is queried on detailed information of a corresponding device according to the device ID, in which the detailed information at least includes an initialization key.

At step S404, after obtaining the detailed information, a list of alternative devices is displayed.

At step S405, an IoT device in the list of alternative devices is determined as the target IoT device according to a selection input of a user, and the BLE connection is established.

For example, the step of establishing the BLE connection between the APP terminal and the target IoT device is explained as follows. The APP terminal searches for a BLE broadcast frame after entering the network configuration process, in which the BLE broadcast frame carries a device ID, a MAC, and an APP ID, for verifying whether the device is a legitimate device and informing address information. With regard to a specific data structure of the BLE broadcast frame, reference can be made to Table 3. After detecting the BLE broadcast frame, the APP terminal at least obtains the device ID and the APP ID carried in the BLE broadcast frame, in which according to the APP ID, it can be determined whether the BLE broadcast frame is sent by a legitimate device that matches the APP terminal. If the BLE broadcast frame matches the APP terminal, the detailed information of the corresponding device is queried from the server according to the device ID. The detailed information at least includes the initialization key, and may also include a write universally unique identifier (Write UUID) for the APP terminal to write data to the IoT device, and a notify universally unique identifier (Notify UUID) for the IoT device

to send data to the APP terminal. After querying the detailed information of the corresponding device, the APP terminal jumps to a search result page and add the device ID of the corresponding device and the above detailed information to the list of alternative devices, so that the user can select the device for which the network configuration needs to be performed from the list.

For example, in the embodiments of the present disclosure, it is required to create product information (the IoT device), register BLE connection information and generate the initialization key on the platform (server). When creating a BLE and Wi-Fi product, device BLE related information needs to be filled in at first, i.e., filling in the Write UUID for the APP (APP terminal) to write data to the IoT device, and the Notify UUID for the IoT device to send data to the APP terminal. After creating the product is finished, the platform obtains a product ID (device ID) and the initialization key for verifying a connection permission.

It is noted that when a plurality of legitimate devices are searched, it is preferred to arrange them according to the device IDs. After receiving the selection input of the user, the IoT device corresponding to the selection input in the list of alternative devices is determined as the target IoT device, and the BLE connection can be established with the IoT device. For example, based on the searched BLE broadcast frame, in the case of network configuration, the APP terminal only needs to enter a searching page, and after the IoT device is searched, by clicking a “network configuration button”, the APP terminal may connect and send the SSID and the password of the router. Therefore, the process of network configuration is simple.

Table 3

MAC（4byte）	device ID（4byte）	APP ID（4byte）

A frame header is a 6-byte Bluetooth MAC of the IoT device. A middle portion is the device ID that is set when the device is created, which is filled in hexadecimal, and the high-bit is padded with zero. An end portion is the APP ID, which is a 4-byte fixed character string.

In some embodiments, based on the above method, the method further includes:

in response to determining that the BLE broadcast frame does not match the APP terminal according to the APP ID or in response to the detailed information being not queried, discarding the BLE broadcast frame; and

in response to the list of alternative devices being not displayed within a first preset duration, displaying second information indicating a search failure.

In the embodiment of the present disclosure, after whether the BLE broadcast frame matches

the APP terminal is determined according to the APP ID, if a determination result is that the BLE broadcast frame does not match the APP terminal, or the detailed information of the corresponding device cannot be obtained after the detailed information of the corresponding device is queried from the server according to the device ID, it is determined that the device corresponding to the BLE broadcast frame is not a legitimate device with respect to the APP terminal. In this case, the BLE broadcast frame is discarded, which is conducive to ensuring the network configuration success rate.

In addition, if the list of alternative devices is not displayed within the first preset duration after searching, it indicates that no qualified device that satisfies the conditions is found within the first preset duration. In this case, the APP terminal jumps to a search failure page, to prompt the user that the device search is failed, so as to facilitate the user to check the devices, which can ensure the user experience and facilitate timely discovery and correction of problems.

In some embodiments, based on the above method, before searching for the BLE broadcast frame, the method further includes:

determining a SSID and a connection password of a router to be connected according to user input.

In the embodiment of the present disclosure, the APP terminal determines the SSID and the corresponding connection password of the router to be connected according to the user input before searching for the BLE broadcast frame, so that after the BLE broadcast frame is found, it is sent to the target IoT device as part of the encrypted network configuration information for network configuration.

In some embodiments, based on the above method, after sending the session key request message to the target IoT device in one or more packets according to the communication data protocol and the packetizing protocol, the method further includes:

in response to receiving initialization key verification failure information returned by the target IoT device, displaying third information indicating a network configuration failure.

In the embodiment of the present disclosure, after sending the session key request message to the target IoT device by packetizing, if the initialization key verification failure information returned by the target IoT device is received, it is determined that the initialization key with respect to the target IoT device in the session key request message sent by the APP terminal to the target IoT device is incorrect, and the current target no-IoT device is not a legitimate device,

so that the third information indicating the network configuration failure is displayed to inform the user to deal with it in time.

In some embodiments, based on the above method, after querying the server on whether the network configuration binding is successful by polling, the method further includes:

in response to not obtaining result information related to the target IoT device by polling within a second preset duration, displaying fourth information indicating a network configuration binding failure.

In the embodiment of the present disclosure, after querying the server on whether the network configuration binding is successful by polling, in response to not obtaining result information related to the target IoT device by polling within the second preset duration, it is determined that the target IoT device is unable to complete the network configuration, or it is unable to complete the network configuration within a specified duration. At this time the fourth information indicating the network configuration binding failure is displayed, to inform the user to deal with it in time.

FIG. 5 is a schematic flowchart of a method for configuring a network for a dual-mode IoT device applied to an IoT device provided by an embodiment of the present disclosure. The method includes the following steps.

At step S501, a BLE connection is established with an APP terminal.

At step S502, after establishing the BLE connection, a session key request message sent in one or more packets by the APP terminal according to a preset communication data protocol and a packetizing protocol is received.

At step S503, the session key request message is assembled according to the packetizing protocol, and the assembled message is split according to the communication data protocol to obtain an initialization key related to the IoT device.

At step S504, the initialization key is verified, and a session key is fed back in response to a successful verification.

At step S505, after receiving encrypted network configuration information that is encrypted according to the session key and sent by the APP terminal, network configuration binding is performed according to the encrypted network configuration information.

A method for configuring a network applied to an IoT device is provided in the embodiment of the present disclosure. The method includes: establishing a BLE connection with an APP

terminal; after establishing the BLE connection, receiving a session key request message sent in one or more packets by the APP terminal according to a preset communication data protocol and a packetizing protocol; obtaining data information carried in the message by assembling the session key request message according to the packetizing protocol and splitting the assembled message according to the communication data protocol, in which the data information includes but is not limited to an initialization key related to the IoT device; after obtaining the initialization key, verifying the initialization key based on the initialization key stored on itself; in response to the verification being successful, determining that the message is a message corresponding to the device, and generating and feeding back a session key to the APP terminal based on the message, for encrypted communication with the APP terminal; and after receiving the encrypted network configuration information encrypted according to the session key sent by the APP terminal, performing network configuration binding according to the encrypted network configuration information, e.g., obtaining the network configuration information by decrypting the encrypted network configuration information according to the session key, and performing network configuration according to the network configuration information.

In conclusion, in the embodiments of the present disclosure, the network configuration information is sent by the point-to-point connection via the BLE connection, rather than the broadcasting method, the multicasting method and other inefficient sending methods. Therefore, the method of the embodiments of the present disclosure has the advantages of a high transmission efficiency, a short configuration duration, and a high network configuration success rate. Encrypting the network configuration information based on the session key is conducive to improving data security of the network configuration. Data compilation based on the application-layer-based data communication protocol is no longer bound to the underlying capabilities of chips, which makes it effective for the chips of different manufacturers. Packetizing based on the data type is no longer specific to the corresponding functions of data, which makes the method of the present disclosure universally applicable.

As illustrated in FIG. 6, in some embodiments, based on the above method, performing network configuration binding according to the encrypted network configuration information includes the following steps.

At step S601, the encrypted network configuration information is decrypted according to the session key, to obtain network configuration binding token information, a SSID and a connection

password of a router, and a reception success signal is sent to the APP terminal.

At step S602, a networking request is sent to the corresponding router according to the SSID and the connection password of the router.

At step S603, after successful networking, a registration or login request is sent to a server according to the network configuration binding token information.

In the embodiment of the present disclosure, the steps of performing network configuration binding according to the encrypted network configuration information includes: obtaining the network configuration information by decrypting the encrypted network configuration information according to the generated session key, in which the network configuration information includes, but is not limited to, network configuration binding token information, a SSID and a connection password of a router; sending a networking request to the corresponding router according to the SSID and the connection password of the router for connecting; and, if the networking is successful, initiating a registration or login request to the server according to the network configuration binding token information, for binding the device under the user name of the APP terminal or logging-in.

Preferably, based on the above method, before establishing the BLE connection with the APP terminal, the method further includes:

after entering a network configuration state, sending a BLE broadcast frame carrying a device ID, a MAC, and an APP ID according to a preset format.

In the embodiment of the present disclosure, before the IoT device establishes the BLE connection with the APP terminal, after entering the network configuration state, the IoT device sends the BLE broadcast frame carrying the device ID, the MAC, and the APP ID according to a preset format, so as to facilitate search, identification, and connection of the APP terminal by the user within a communication range.

FIG. 7 is a schematic flowchart of a method for configuring a network for a dual-mode IoT device which is applied to a server provided by an embodiment of the present disclosure. The method includes the following steps.

At step S701, after receiving a request for network configuration binding token information sent by an APP terminal, the network configuration binding token information is fed back to the APP terminal.

At step S702, in response to receiving a registration or login request sent by the IoT device

after successful networking, a verification is performed according to the network configuration binding token information carried in the registration or login request.

At step S703, a registration or login process of the IoT device is performed in response to a successful verification, and the IoT device is bound under a user name of the APP terminal.

In the embodiment of the present disclosure, a network configuration method applied to a server is provided. After receiving the request for the network configuration binding token information from the APP terminal with which it is connected communicatively, the server feeds back the network configuration binding token information for subsequent verification and legal confirmation. If the server receives the registration or login request sent by the IoT device after it is successfully networked, the server verifies the registration or login request according to the network configuration binding token information carried in the request. If the network configuration binding token information carried in the request is the same as or matches the network configuration binding token information sent to the APP terminal, it is determined that the IoT device is a device corresponding to the APP terminal. The IoT device is registered or logged in, and the IoT device is bound under a user name of the APP terminal. Preferably, a binding operation may be performed only at the time of registration.

In some embodiments, based on the above method, after performing the registration or login process of the IoT device after successful verification, and binding the IoT device under the user name of the APP terminal, the method further includes:

feeding back network configuration binding success information based on a polling request on whether network configuration binding is successful sent by the APP terminal.

In the embodiment of the present disclosure, after performing the registration or login process of the IoT device, and binding the IoT device under the user name of the APP terminal, if the server receives a polling request on whether the network configuration binding is successful sent from the APP terminal, the server feeds back network configuration binding success information to the APP terminal, to inform the user of the information accurately.

It is noted that when the server does not receive the registration or login request sent by the IoT device, or, does not complete the registration or login process according to such registration or login request, if the server receives the above polling request sent by the APP terminal, the server does not feed back the information.

FIG. 8 is a schematic flowchart of an illustrative method for configuring a network for a

dual-mode IoT device provided by an embodiment of the present disclosure. FIG. 8 includes the following illustrative steps. (1) The IoT device enters a network configuration state and sends a broadcast frame (BLE broadcast frame) carrying a product ID (device ID), a Mac (MAC), and ID (APP ID) according to a specified format. (2) The APP (APP terminal) enters a network configuration process by selecting the SSID of the router to be connected and entering the password (connection password). (3) The APP jumps to a searching page and searches for the BLE broadcast frame. (4) After detects the BLE broadcast frame, the APP extracts the product ID, Mac, ID, and etc. in the BLE broadcast frame, and verifies the ID and discards it if it does not match with the APP. (5) The APP queries the platform (server) for detailed information of the product (IoT device) using the product ID after verifying the ID. (6) The platform returns the detailed information of the product to the APP, including BLE-related Write UUID, Notify UUID, and the initialization key. After querying the detailed information of the product, the APP jumps to a search result page and display a device list (the list of alternative devices). If it fails to find any detailed information of the product, it means that the product corresponding to the product ID is not a legal product of the platform, and the APP discards the broadcast frame. If no qualified device (target IoT device) is found after 180s, the APP jumps to a search failure page, to prompt the user that the search has failed and the devices need to be checked. (7) The user selects the device for network configuration, and the APP first establishes the BLE connection with the device. After the connection is successful, the APP uses the data protocol (preset communication data protocol) to carry the initialization key to send a session key request message to the device in one or more packets. (8) The device receives and assembles message based on the packetizing protocol, disassembles the initialization key based on the data protocol, and verifies the initialization key. If the verification is succeed, the device feeds back the generated session key, and if the verification is failed, the device replies with an error code that the verification is failed. (9) If the APP receives the session key, the APP initiates a request for network configuration binding token information to the platform. If the APP receives the error code, the APP displays the information that the network configuration of the device is failed. (10) The platform returns the network configuration binding token information to the APP. (11) The APP uses the received session key to encrypt the SSID and the password of the router, and the network configuration binding token information from the platform, and then sends the encrypted network configuration information to the device. (12) After receives the network configuration information, the device

decrypts it using the session key and replies a network configuration information success message to the APP. (13) After confirms that the device receives the network configuration information, the APP initiates the operation of querying the platform whether the network configuration is successful and whether it is bound to the user name of the APP (network configuration binding). If there is no result related to the device after 180s, the APP prompts the user that the network configuration binding is failed (the fourth information). (14) The device uses the SSID and the password of the router for networking. (15) If the networking is succeed, the APP uses the network configuration binding token information to initiate registration and login operations on the platform. If the networking is failed, the APP also is informed of network configuration binding failure due to polling timeout, and not in a waiting state to make the process abnormal. (16) After the registration and login operations of the device are completed on the platform, the platform binds the device under the user name of the APP and inform the APP of network configuration binding success in response to the polling request of the APP (via the network configuration binding success information). (17) The APP display the first message indicating that the network configuration binding is successful, and the process is completed. It is understood that the complete and enforceable network configuration process provided by the embodiments of the present disclosure adopts a network search and configuration method, which is simple to operate and highly efficient. For the device in the embodiments of the present disclosure, as long as it is a dual-mode BLE and Wi-Fi chip, the network configuration can be performed for it according to the network configuration process of the embodiments of the present disclosure. Decoding is performed in the BLE application layer of the device, which is not strongly correlated with the BLE underlying driver, and is simple to adapt and has high universality.

Referring to FIG. 9, an APP terminal is provided by an embodiment of the present disclosure. The APP includes:

a first processing module 901, configured to establish a BLE connection with a target IoT device;

a second processing module 902, configured to, after establishing the BLE connection, send a session key request message to the target IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, in which a data structure of the communication data protocol includes: an operation code, a function point ID, and function point data;

a third processing module 903, configured to, after receiving a session key returned by the target IoT device, generate encrypted network configuration information based on the session key; and

a fourth processing module 904, configured to send the encrypted network configuration information to the target IoT device, so that the target IoT device performs network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above APP terminal, the third processing module includes:

a first processing sub-module, configured to send a request for network configuration binding token information to a server; and

a second processing sub-module, configured to, after receiving the network configuration binding token information fed back by the server, encrypt the network configuration binding token information, a pre-determined SSID and a connection password of a router according to the session key, to generate the encrypted network configuration information.

In some embodiments, the above APP terminal further includes:

a thirteenth processing module, configured to, after determining that the target IoT device receives the encrypted network configuration information, query a server on whether the network configuration binding is successful by polling; and

a fourteenth processing module, configured to, after receiving network configuration binding success information fed back by the server, display first information indicating that the network configuration binding is successful.

In some embodiments, based on the above APP terminal, the first processing module includes:

a third processing sub-module, configured to search for a BLE broadcast frame, in which the BLE broadcast frame carries a device ID, a MAC, and an APP ID;

a fourth processing sub-module, configured to, in response to detecting the BLE broadcast frame, determine whether the BLE broadcast frame matches the APP terminal according to the APP ID;

a fifth processing sub-module, configured to, in response to determining that the BLE broadcast frame matches the APP terminal, query the server on detailed information of a corresponding device according to the device ID, in which the detailed information at least includes an initialization key;

a sixth processing sub-module, configured to, after obtaining the detailed information, display a list of alternative devices; and

a seventh processing sub-module, configured to determine an IoT device in the list of alternative devices as the target IoT device according to a selection input of a user, and establish the BLE connection.

In some embodiments, the above APP terminal further includes:

a fifteenth processing module, configured to, in response to determining that the BLE broadcast frame does not match the APP terminal according to the APP ID or in response to not obtaining the detailed information, discard the BLE broadcast frame; and

a sixteenth processing module, configured to, in response to determining that the list of the alternative devices is not displayed within a first preset duration, display second information indicating a search failure.

In some embodiments, before searching for the BLE broadcast frame, the above APP terminal further includes:

a seventeenth processing module, configured to determine the SSID and the connection password of a router to be connected according to user input.

In some embodiments, the above APP terminal further includes:

an eighteenth processing module, configured to, in response to receiving initialization key verification failure information returned by the target IoT device, display third information indicating a network configuration failure.

In some embodiments, the above APP terminal further includes:

a nineteenth processing module, configured to, in response to not obtaining result information related to the target IoT device by polling within a second preset duration, display fourth information indicating a network configuration binding failure.

The embodiment of the APP terminal of the embodiments of the present disclosure is an apparatus corresponding to the above embodiment of the method for configuring a network for a dual-mode IoT device applied to an APP terminal. All the implementation means in the above method embodiments are applicable in the embodiment of the APP terminal, to achieve the same technical effects.

As illustrated in FIG. 10, an IoT device is provided in the embodiment of the present disclosure. The IoT device includes:

a fifth processing module 1001, configured to establish a BLE connection with an APP terminal;

a sixth processing module 1002, configured to, after establishing the BLE connection, receive a session key request message sent in one or more a packet by the APP terminal according to a preset communication data protocol and a packetizing protocol;

a seventh processing module 1003, configured to assemble the session key request message based on the packetizing protocol, and split the assembled message according to the communication data protocol to obtain an initialization key of the IoT device;

an eighth processing module 1004, configured to verify the initialization key, and feed back a session key in response to a successful verification; and

a ninth processing module 1005, configured to, after receiving encrypted network configuration information that is encrypted according to the session key and sent by the APP terminal, perform network configuration binding according to the encrypted network configuration information.

In some embodiments, based on the above IoT device, the ninth processing module includes:

an eighth processing sub-module, configured to decrypt the encrypted network configuration information according to the session key, to obtain network configuration binding token information, a SSID and a connection password of a router, and send a reception success signal to the APP terminal;

a ninth processing sub-module, configured to send a networking request to the corresponding router according to the SSID and the connection password of the router; and

a tenth processing sub-module, configured to, after successful networking, send a registration or login request to a server according to the network configuration binding token information.

In some embodiments, the above IoT device further includes:

a twentieth processing module, configured to, after entering a network configuration state, send a BLE broadcast frame carrying a device ID, a MAC, and an APP ID according to a preset format.

The embodiment of the IoT device of the embodiments of the present disclosure is an apparatus corresponding to the above embodiments of the method for configuring a network for a dual-mode IoT device applied to an IoT device. All the implementation means in the above method embodiments are applicable in the embodiment of the IoT device, to achieve the same

technical effects.

As illustrated in FIG. 11, a server is provided in the embodiment of the present disclosure. The server includes:

a tenth processing module 1101, configured to, after receiving a request for network configuration binding token information sent by an APP terminal, send the network configuration binding token information to the APP terminal;

an eleventh processing module 1102, configured to, in response to receiving a registration or login request sent by the IoT device after successful networking, perform a verification according to the network configuration binding token information carried in the registration or login request; and

a twelfth processing module 1103, configured to perform a registration or login process of the IoT device in response to a successful verification, and bind the IoT device under a user name of the APP terminal.

In some embodiments, the above server further includes:

a twenty-first processing module, configured to feed back network configuration binding success information in response to a polling request on whether network configuration binding is successful sent by the APP terminal.

The embodiment of the server of the embodiments of the present disclosure is an apparatus corresponding to the above embodiments of the method for configuring a network for a dual-mode IoT device applied to a server. All the implementation means in the above method embodiments are applicable in the embodiment of the server, to achieve the same technical effects.

A computer-readable storage medium having computer programs stored thereon is provided in the embodiments of the present disclosure. When the computer programs are executed by a processor, the steps of the method for configuring a network for a dual-mode IoT device applied to an APP terminal, or the steps of the method for configuring a network for a dual-mode IoT device applied to an IoT device, or the steps of the method for configuring a network for a dual-mode IoT device applied to a server are implemented.

In addition, repeated reference numerals and/or letters are used in various examples of the present disclosure for the purposes of simplicity and clarity. These reference numerals and/or letters do not indicate relations between the embodiments and/or settings discussed. It should also be noted that in this present disclosure, relational terms, such as “first” and “second”, are used

only to distinguish one entity or operation from another, and do not necessarily require or imply any such actual relation or order between these entities or operations. Moreover, the terms “includes”, “comprises” or any other variant thereof are intended to cover non-exclusive inclusion.

The present disclosure only include optional embodiments of the present disclosure. It should be noted that for those skilled in the art, a number of improvements and embellishments may be made without departing from the principles described in the present disclosure, and these improvements and embellishments should also be regarded as within the scope of protection of the present disclosure.

WHAT IS CLAIMED IS:

1. A method for configuring a network for a dual-mode internet of things (IoT) device, performed by an application (APP) terminal, comprising:

establishing a bluetooth low energy (BLE) connection with a target IoT device;

sending a session key request message to the target IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, a data structure of the communication data protocol comprising: an operation code, a function point identifier (ID), and function point data;

receiving a session key returned by the target IoT device;

generating encrypted network configuration information based on the session key; and

sending the encrypted network configuration information to the target IoT device, wherein the encrypted network configuration information is used for the target IoT device to perform network configuration binding.

2. The method of claim 1, wherein generating the encrypted network configuration information based on the session key, comprises:

sending a request for network configuration binding token information to a server;

receiving the network configuration binding token information fed back by the server; and

encrypting the network configuration binding token information, a pre-determined service set identifier (SSID) and a connection password of a router according to the session key, to generate the encrypted network configuration information.

3. The method of claim 1, after sending the encrypted network configuration information to the target IoT device, further comprising:

determining that the target IoT device receives the encrypted network configuration information;

querying a server on whether the network configuration binding is successful by polling; and

in response to receiving network configuration binding success information fed back by the server, displaying first information indicating that the network configuration binding is successful.

4. The method of claim 1, before establishing the BLE connection with the target IoT device, further comprising:

searching for a BLE broadcast frame, wherein the BLE broadcast frame carries a device ID, a media access control (MAC), and an APP ID;

in response to detecting the BLE broadcast frame, determining whether the BLE broadcast frame matches the APP terminal according to the APP ID;

in response to determining that the BLE broadcast frame matches the APP terminal, querying the server on detailed information of a corresponding device according to the device ID, wherein the detailed information at least comprises an initialization key;

displaying a list of alternative devices based on the detailed information; and

determining an IoT device in the list of alternative devices as the target IoT device according to a selection input of a user.

5. The method of claim 4, further comprising:

in response to determining that the BLE broadcast frame does not match the APP terminal according to the APP ID or in response to not obtaining the detailed information, discarding the BLE broadcast frame; and

in response to determining that the list of alternative devices is not displayed within a first preset duration, displaying second information indicating a search failure.

6. The method of claim 4, before searching for the BLE broadcast frame, further comprising:

determining an SSID and a connection password of a router to be connected according to a user input.

7. The method of claim 1, after sending the session key request message to the target IoT device in one or more packets according to the communication data protocol and the packetizing protocol, further comprising:

in response to receiving initialization key verification failure information returned by the target IoT device, displaying third information indicating a network configuration failure.

8. The method of claim 3, after querying the server on whether the network configuration binding is successful by polling, further comprising:

in response to not obtaining result information related to the target IoT device by polling within a second preset duration, displaying fourth information indicating a network configuration binding failure.

9. A method for configuring a network for a dual-mode internet of things (IoT) device, performed by an IoT device, comprising:

establishing a bluetooth low energy (BLE) connection with an application (APP) terminal;

receiving a session key request message sent in one or more packets by the APP terminal

according to a preset communication data protocol and a packetizing protocol;

assembling the session key request message according to the packetizing protocol, and splitting an assembled message according to the communication data protocol to obtain an initialization key of the IoT device;

verifying the initialization key, and feeding back a session key in response to a successful verification; and

receiving encrypted network configuration information that is encrypted according to the session key and sent by the APP terminal; and

performing network configuration binding according to the encrypted network configuration information.

10. The method of claim 9, wherein performing the network configuration binding according to the encrypted network configuration information, comprises:

decrypting the encrypted network configuration information according to the session key, to obtain network configuration binding token information, a service set identifier (SSID) and a connection password of a router, and sending a reception success signal to the APP terminal;

sending a networking request to the corresponding router according to the SSID and the connection password of the router; and

after successful networking, sending a registration or login request to a server according to the network configuration binding token information.

11. The method of claim 9, before establishing the BLE connection with the APP terminal, further comprising:

entering a network configuration state; and

sending a BLE broadcast frame carrying a device ID, a media access control (MAC), and an APP ID according to a preset format.

12. A method for configuring a network for a dual-mode internet of things (IoT) device, performed by a server, comprising:

receiving a request for network configuration binding token information sent by an application (APP) terminal;

sending the network configuration binding token information to the APP terminal;

in response to receiving a registration or login request sent by the IoT device after successful networking, performing a verification according to the network configuration binding token

information carried in the registration or login request; and

performing a registration or login process of the IoT device in response to a successful verification, and binding the IoT device under a user name of the APP terminal.

13. The method of claim 12, after performing the registration or login process of the IoT device in response to the successful verification, and binding the IoT device under the user name of the APP terminal, further comprising:

feeding back network configuration binding success information based on a polling request on whether network configuration binding is successful sent by the APP terminal.

14. An application (APP) terminal, comprising:

a first processing module, configured to establish a bluetooth low energy (BLE) connection with a target internet of things (IoT) device;

a second processing module, configured to send a session key request message to the target IoT device in one or more packets according to a preset communication data protocol and a packetizing protocol, a data structure of the communication data protocol comprising: an operation code, a function point identifier (ID), and function point data;

a third processing module, configured to receive a session key returned by the target IoT device, and generate encrypted network configuration information based on the session key; and

a fourth processing module, configured to send the encrypted network configuration information to the target IoT device, wherein the encrypted network configuration information is used for the target IoT device to perform network configuration binding.

15. An IoT device, comprising:

a fifth processing module, configured to establish a bluetooth low energy (BLE)connection with an application (APP)terminal;

a sixth processing module, configured to receive a session key request message sent by the APP terminal according to a preset communication data protocol and a packetizing protocol;

a seventh processing module, configured to assemble the session key request message according to the packetizing protocol, and split the assembled message according to the communication data protocol to obtain an initialization key of the IoT device;

an eighth processing module, configured to verify the initialization key, and feed back a session key in response to a successful verification; and

a ninth processing module, configured to receive encrypted network configuration

information that is encrypted according to the session key and sent by the APP terminal, and perform network configuration binding according to the encrypted network configuration information.

16. A server, comprising:

a tenth processing module, configured to receive a request for network configuration binding token information sent by an application (APP) terminal, and send the network configuration binding token information to the APP terminal;

an eleventh processing module, configured to, in response to receiving a registration or login request sent by an internet of things (IoT) device after successful networking, perform a verification according to the network configuration binding token information carried in the registration or login request; and

a twelfth processing module, configured to perform a registration or login process of the IoT device in response to a successful verification, and bind the IoT device under a user name of the APP terminal.

17. A computer-readable storage medium having computer programs stored thereon, wherein when the computer programs are executed by a processor, the steps of the method for configuring a network for a dual-mode internet of things (IoT) device applied to an APP terminal of any one of claims 1-8, or the steps of the method for configuring a network for a dual-mode IoT device applied to an IoT device of any one of claims 9-11, or the steps of the method for configuring a network for a dual-mode IoT device applied to a server of claim 12 or 13 are implemented.