

METHOD AND SYSTEM FOR ACCESSING A NETWORK HOTSPOT DEVICE BY AN UNCONFIGURED DEVICE

[1] The present application claims priority to Chinese Patent Application No. 201810098029.6 filed on January 31, 2018, entitled “a method and system for accessing a network hotspot device by an unconfigured device”, of which the entire contents are incorporated in this application by reference.

TECHNICAL FIELD

[2] The present application relates to communication technologies, and particularly to a method for accessing a network hotspot device by an unconfigured device and system for accessing a network hotspot device by an unconfigured device.

BACKGROUND

[3] With the development of the Internet of Things, more and more smart devices use Wi-Fi to access home routers to realize functions such as remote device control and scene linkage in smart home scenarios.

[4] Before accessing to the Internet, smart devices need to obtain Service Set Identifier (SSID) and a password of a router based on network configuration schemes to access the Internet. The current configuration scheme is mainly realized by Wi-Fi or Bluetooth.

[5] Regardless of whether it is by means of Wi-Fi or Bluetooth, the user needs to manually enter the SSID and the password during the network configuration. There is a risk of input errors. After a user updates access information of the router, the smart device connected to the router requires the user to configure the smart device again, which negatively affect the user experience.

SUMMARY

[6] In view of the above problems, embodiments of the present application are provided to provide a method for accessing a network hotspot device by an unconfigured device and a corresponding system for accessing a network hotspot device by an unconfigured device to overcome the above problems or at least partially solve the above problems.

[7] In order to solve the above problems, embodiments of the present application provide a method for accessing a network hotspot device by an unconfigured device, wherein, the network hotspot device creates a first hotspot and a second hotspot, the method comprising: after the first access information of the first hotspot been updated, disconnecting, by the network hotspot device, a connection between the unconfigured device that has accessed the network hotspot device through the first hotspot and the first hotspot of the network hotspot device; accessing, by the unconfigured device, the second hotspot; sending, by the network hotspot device, the updated first access information to the unconfigured device through the second hotspot; and accessing, by the unconfigured device, the first hotspot using the first access information.

[8] Preferably, after sending, by the network hotspot device, the updated first access information to the unconfigured device through the second hotspot comprises:

[9] receiving, by the network hotspot device, device information of the unconfigured device sent by the unconfigured device through the second hotspot;

[10] encrypting, by the network hotspot device, the updated first access information with the device information and sending the encrypted first access information to the unconfigured device.

[11] Preferably, the step of accessing, by the unconfigured device, the first hotspot using the first access information comprises:

[12] decrypting, by the unconfigured device, the encrypted first access information using the device information and accessing the first hotspot using the decrypted first access information.

[13] Preferably, the step of receiving, by the network hotspot device, the device information of the unconfigured device sent by the unconfigured device through the second hotspot comprises:

[14] determining, by the network hotspot device, whether the unconfigured device is in a preset white list; and

[15] if the unconfigured device being in the preset white list, accepting, by the network hotspot device, the device information sent by the unconfigured device.

[16] Preferably, further comprising:

[17] if the unconfigured device not being in the preset white list, disconnecting, by the network hotspot device, a connection between the unconfigured device and the second hotspot.

[18] Preferably, the step of encrypting, by the network hotspot device, the updated first access information with the device information comprises:

[19] generating, by the network hotspot device, an encryption key using the device information; and

[20] encrypting, by the network hotspot device, the updated first access information using the encryption key according to a preset symmetric encryption algorithm.

[21] Preferably, the step of decrypting, by the unconfigured device, the encrypted first access information using the device information comprises:

[22] generating, by the unconfigured device, a decryption key using the device information;

[23] decrypting, by the unconfigured device, the encrypted first access information using the decryption key according to an inverse algorithm corresponding to the symmetric encryption algorithm.

[24] Preferably, further comprising:

[25] receiving, by the network hotspot device, the preset white list from a server.

[26] Preferably, further comprising:

[27] after the unconfigured device accessing to the first hotspot at the first time, adding, by the network hotspot device, the unconfigured device to the preset white list.

[28] Preferably, the step of accessing, by the unconfigured device, the second hotspot comprises:

[29] accessing, by the unconfigured device, the second hotspot using preset second access information for the second hotspot.

[30] Embodiments of the present application also disclose a system for accessing a network hotspot device by an unconfigured device, characterized in, comprising: a unconfigured device and a network hotspot device, wherein

[31] the network hotspot device is used to create a first hotspot and a second hotspot and to disconnect a connection between the unconfigured device that has accessed the network hotspot device through the first hotspot and the first hotspot of the network hotspot device after first access information of the first hotspot having been updated,

[32] the unconfigured device is used to access the second hotspot,

[33] the network hotspot device is used to send the updated first access information to the unconfigured device through the second hotspot, and

[34] the unconfigured device is used to access the first hotspot using the first access information.

[35] Preferably, the network hotspot device is further used to receive device information of the unconfigured device sent by the unconfigured device through the second hotspot, to encrypt the updated first access information with the device information, and to send the encrypted first access information to the unconfigured device.

[36] Preferably, the unconfigured device is further used to decrypt the encrypted first access information using the device information and to access the first hotspot using the decrypted first access information.

[37] Preferably, the network hotspot device is used to determine whether the unconfigured device is in a preset white list and to accept the device information sent by the unconfigured device if the unconfigured device is in the preset white list.

[38] Preferably, the network hotspot device is further used to disconnect a connection between the unconfigured device and the second hotspot if the unconfigured device is not in the preset white list.

[39] Preferably, the network hotspot device is further used to generate an encryption key using the device information and to encrypt the updated first access information using the encryption key according to a preset symmetric encryption algorithm.

[40] Preferably, the unconfigured device is further used to generate a decryption key using the device information and decrypt the encrypted first access information using the decryption key according to an inverse algorithm corresponding to the symmetric encryption algorithm.

[41] Preferably, the system further comprises a server:

[42] the network hotspot device is further used to receive the preset white list from a server.

[43] Preferably, the network hotspot device is further used to add the unconfigured device to the preset white list after the unconfigured device accesses to the first hotspot at the first time.

[44] Preferably, the unconfigured device is further used to access the second hotspot using preset second access information for the second hotspot.

[45] The embodiments of the present application also disclose an apparatus for accessing a network hotspot device by an unconfigured device, characterized in, comprising:

[46] one or more processors; and

[47] one or more machine-readable media having stored thereon instructions that, when executed by the one or more processors, cause the apparatus to perform one or more of the methods described in claims 1-10.

[48] The embodiments of the present application also disclose one or more machine-readable medium having stored thereon instructions that, when executed by one or more processors, cause an apparatus to perform one or more of the methods described in claims 1-10.

[49] The embodiments of the present application include the following advantages:

[50] In the embodiments of the present application, when the user has updated the access information of the Internet hotspot of the network hotspot device, causing the unconfigured device to be disconnected, the network to be distributed device can access the discovery hotspot of the network hotspot device. The network hotspot device may send the updated access information of the Internet hotspot to the unconfigured device through the discovery hotspot. The unconfigured device uses the access information to access the Internet hotspot of the network hotspot device.

[51] The embodiments of the present application solves the problem that network configuration of devices is repeated after the access information of an Internet hotspot is updated, the whole process is transparent to users, does not need user participation and has very good user experience.

BRIEF DESCRIPTION OF THE DRAWINGS

[52] **FIG. 1** is a step flow chart of embodiment 1 of a method for accessing a network hotspot device by an unconfigured device of the present application.

[53] **FIG. 2** is a step flow chart of embodiment 2 of a method for accessing a network hotspot device by an unconfigured device of the present application.

[54] **FIG. 3** is a step flow chart of embodiment 3 of a method for accessing a network hotspot device by an unconfigured device of the present application.

[55] **FIG. 4** is a flow chart of accessing a network hotspot device by a smart device of embodiments of the present application.

[56] **FIG. 5** is a structural diagram of embodiments of a system for accessing a network hotspot device by an unconfigured device of the present application.

DETAILED DESCRIPTION

[57] In order to make the above-mentioned objects, features and advantages of the present application more obvious and understandable, the present disclosure will be described in further detail below with reference to the accompanying drawings and specific embodiments.

[58] In an Internet of Things scenario, a router is used to provide WiFi hotspots for smart devices. The router can provide hotspots with Internet

access and hotspots without Internet access. This kind of hotspot with the ability to access the Internet can be called an online hotspot.

[59] Network distribution refers to the process of sending access information of Internet hotspots to smart devices. The access information includes Service Set Identifier (SSID) and password of the hotspot.

[60] When the user updates access information of the hotspot the router, the smart device connected to the router requires the user to configure the smart device again.

[61] **FIG. 1** illustrates a flow chart of an exemplary method for enabling access of an unconfigured device to a network hotspot device, consistent with some embodiments of the present application. The network hotspot creates a first hotspot and a second hotspot. The method can include the following steps.

[62] In step 101, after the first access information of the first hotspot been updated, disabling, by the network hotspot device, a connection between the first hotspot of the network hotspot device and the unconfigured device that has accessed the network hotspot device through the first hotspot.

[63] In the embodiments of the present application, the network hotspot device can be a router or a wireless Access Point (AP) without routing capabilities.

[64] The network hotspot creates a first hotspot and a second hotspot after power-on. The first hotspot is an Internet accessing hotspot that is capable of accessing the Internet. The second hotspot is a discovery hotspot that is not capable of accessing the Internet. If the unconfigured device accesses the first hotspot, the unconfigured device can communicate with the network hotspot device and can also access the Internet through the network hotspot device. If the unconfigured device accesses the second hotspot, the unconfigured device can communicate with the network hotspot device but cannot access the Internet through the network hotspot device.

[65] The unconfigured device uses the first access information (e.g., SSID and password) corresponding to the first hotspot to access the first hotspot. After the user updates the first access information of the first hotspot, the network hotspot device disconnects the unconfigured device from the first hotspot. The step of updating the access information by the user includes: the user creates new access information, and the user modifies the original access information.

[66] In step 102, the unconfigured device accesses the second hotspot.

[67] After the network hotspot device disconnects the unconfigured device from the first hotspot, the unconfigured device again tries to use the old first access information to access the first hotspot, but access failure can occur. The unconfigured device also uses the access information for other Internet hotspots to try to access other Internet hotspots.

[68] After the unconfigured device fails to access the Internet hotspot, the unconfigured device accesses the second hotspot of the network hotspot device.

[69] In step 103, the network hotspot device sends the updated first access information to the unconfigured device through the second hotspot.

[70] In step 104, the unconfigured device accesses the first hotspot using the updated first access information.

[71] The unconfigured device receives the first access information sent by the network hotspot device through the second hotspot, and then the unconfigured device disconnects from the second hotspot and uses the decrypted first access information to re-access the first hotspot.

[72] In some embodiments, the user updates the access information of the Internet hotspot of the network hotspot device, causing the unconfigured device to be disconnected, the unconfigured device can access the discovery hotspot of the network hotspot device. The network hotspot device can send the updated access information of the

Internet hotspot to the unconfigured device through the discover hotspot. The unconfigured device can access the Internet access hotspot of the network hotspot device using the access information.

[73] The embodiments of the present application provide solutions to the issue of repeated network configuration of the device after the access information of the Internet hotspot being updated. The entire process is transparent to users, does not require user participation, and has a very good user experience.

[74] **FIG. 2** illustrates a step flow chart of embodiment 2 of a method for accessing a network hotspot device by an unconfigured device of the present application. The network hotspot creates a first hotspot and a second hotspot. The method can include the following steps.

[75] In step 201, after the first access information of the first hotspot been updated, disabling, by the network hotspot device, a connection between the first hotspot of the network hotspot device and the unconfigured device that has accessed the network hotspot device through the first hotspot.

[76] In the embodiments of the present application, the network hotspot device can be a router or a wireless Access Point (AP) without routing capabilities.

[77] The network hotspot creates a first hotspot and a second hotspot after power-on. The first hotspot is an Internet accessing hotspot that is capable of accessing the Internet. The second hotspot is a discovery hotspot that is not capable of accessing the Internet. If the unconfigured device accesses the first hotspot, the unconfigured device can communicate with the network hotspot device and can also access the Internet through the network hotspot device. If the unconfigured device accesses the second hotspot, the unconfigured device can communicate with the network hotspot device but cannot access the Internet through the network hotspot device.

[78] The unconfigured device uses the first access information (e.g., SSID and password) corresponding to the first hotspot to access the first hotspot. After the user updates the first access information of the first hotspot, the network hotspot device disconnects the unconfigured device from the first hotspot.

[79] In step 202, the unconfigured device accesses the second hotspot.

[80] After the network hotspot device disconnects the unconfigured device from the first hotspot, the unconfigured device again tries to use the old first access information to access the first hotspot, but access failure can occur. The unconfigured device also uses the access information for other Internet hotspots to try to access other Internet hotspots.

[81] After the unconfigured device fails to access the Internet hotspot, the unconfigured device accesses the second hotspot of the network hotspot device.

[82] In step 203, the network hotspot device obtains device information sent by the unconfigured device through the second hotspot.

[83] When the unconfigured device accesses the second hotspot, the unconfigured device can send its own device information to the network hotspot device through the second hotspot. Device information can include the device's MAC address, random number, and other data defined by the manufacturer of the device (such as device name and device key).

[84] In step 204, the network hotspot device uses the device information to encrypt the updated first access information and sends the encrypted first access information to the unconfigured device.

[85] The network hotspot device can use the device information to encrypt the updated first access information and send the encrypted first access information to the unconfigured device.

[86] In step 205, the unconfigured device uses the device information to decrypt the encrypted first access information and uses the decrypted first access information to access the first hotspot.

[87] The unconfigured device receives the encrypted first access information sent by the network hotspot device through the second hotspot, and then uses its own device information to decrypt the encrypted first access information. Then, the unconfigured device disconnects the second hotspot and uses the decrypted first access information to re-access the first hotspot.

[88] In some embodiments of the present application, when the user updates the access information of the Internet accessing hotspot of the network hotspot device, resulting in the offline connection the unconfigured device , it can access the discovery hotspot of the network hotspot device. Device information is sent to the network hotspot device through the discovery hotspot. The network hotspot device uses the device information to encrypt the updated access information of the Internet accessing hotspot, and then sends the encrypted access information to the unconfigured device. The unconfigured device uses its own device information to decrypt the encrypted access information, and then uses the access information to access the Internet accessing hotspot of the network hotspot device.

[89] The embodiments of the present application solves the problem of repeated network configuration of the device after the access information of the Internet hotspot being updated. The entire process is transparent to users, does not require user participation, and has a very good user experience. The entire process uses encryption measures to ensure data security, and uses device information for encryption, which can ensure the uniqueness of encryption for different devices and has a high security level.

[90] **FIG. 3** illustrates step flow chart of embodiment 3 of a method for accessing a network hotspot device by an unconfigured device of the present application. The network hotspot creates a first hotspot and a second hotspot. The method can include the following steps.

[91] In step 301, after the first access information of the first hotspot been updated, disabling, by the network hotspot device, a connection between the first hotspot of the network hotspot device and the unconfigured device that has accessed the network hotspot device through the first hotspot.

[92] The network hotspot creates a first hotspot and a second hotspot after power-on.

[93] After the user updates the first access information of the first hotspot, the network hotspot device disconnects the unconfigured device from the first hotspot.

[94] In the embodiments of the present application, step 302 can include:

[95] The unconfigured device accesses the second hotspot using preset second access information for the second hotspot.

[96] In the embodiments of the present application, the second access information (including SSID and password) of the second hotspot of the network hotspot device is fixed. In the unconfigured device, the second hotspot access information of the network hotspot device can be preset. When the unconfigured device cannot access the Internet hotspot, the unconfigured device accesses the second hotspot of the network hotspot device using the preset second access information.

[97] In step 303, the network hotspot device determines whether the unconfigured device is in a preset white list.

[98] The white list records the list of unconfigured devices that are allowed to access the first hotspot. If the unconfigured device is in the white list, the network hotspot

device performs the process of sending the first access information to unconfigured device; if the unconfigured device is not in the white list, the network hotspot device does not send the first access information to the unconfigured device.

[99] The white list can be stored locally on the network hotspot device. Preferably, the white list can also be stored in the server. Storing the white list in the server can prevent the white list from being leaked due to local attacks. In some embodiments of the present application, the method can further include: the network hotspot device receives a preset white list sent by the server.

[100] In some embodiments of the present application, the unconfigured devices in the white list can also be configured by the user or can be added by the network hotspot device itself.

[101] In the embodiments of the present application, the method can further include:

[102] After the network hotspot device accesses the first hot spot for the first time, the network hotspot device adds the network hotspot device to the preset white list.

[103] Specifically, after the device to be allocated network uses the first access information to access the first hotspot of the network hotspot device, the network hotspot device can add the device to be allocated to the white list.

[104] In step 304, if the unconfigured device is in the preset white list, the network hotspot receives the device information sent by the unconfigured device.

[105] In the embodiments of the present application, after the unconfigured device accesses the second hotspot, the unconfigured device can send its own device information to the network hotspot device through the second hotspot. If the unconfigured device is in the white list, the network hotspot device accepts the device information of the unconfigured device.

[106] Specifically, if the unconfigured device is in the preset white list, the network hotspot device can send a device information query request message to the unconfigured device through the second network hotspot. After receiving the device information query request message, the unconfigured device sends the device information to the network hotspot device.

[107] In the embodiments of the present application, the method can further include:

[108] If the unconfigured device is not in the preset white list, the network hotspot device disconnects the unconfigured device from the second hotspot.

[109] Specifically, if the unconfigured device is not in the white list, the network hotspot device does not accept the device information of the unconfigured device and disconnects the unconfigured device from the second hotspot.

[110] In step 305, the network hotspot device uses the device information to encrypt the updated first access information and sends the encrypted first access information to the unconfigured device.

[111] The network hotspot device uses the device information to encrypt the updated first access information and sends the encrypted first access information to the unconfigured device.

[112] In the embodiments of the present application, the step that the network hotspot device uses the device information to encrypt the updated first access information can further include the following sub-steps:

[113] In sub-step S11, the network hotspot device uses the device information to generate an encryption key.

[114] In the embodiments of the present application, the network hotspot device can use the device information to generate an encryption key according to a specific key algorithm.

[115] Specifically, for some symmetric encryption algorithms, the encryption key and the decryption key are required to be a bit string of a specific length. Therefore, it is necessary to generate the encryption key of the specific length according to a specific key algorithm.

[116] In sub-step S12, the network hotspot device uses the encryption key to encrypt the updated first access information according to a preset symmetric encryption algorithm.

[117] The symmetric encryption algorithm refers to an algorithm that the encrypting party and the decrypting party can use the same key for encryption and decryption, for example, Advanced Encryption Standard (AES) symmetric encryption algorithm, RC5 symmetric encryption algorithm.

[118] After the encryption party uses the encryption key to encrypt the data according to the encryption algorithm, the decryption party can use the same decryption key as the encryption key to decrypt the encrypted data according to the inverse algorithm corresponding to the encryption algorithm.

[119] In step 306, the unconfigured device uses the device information to decrypt the encrypted first access information and uses the decrypted first access information to access the first hotspot.

[120] In the embodiments of the present application, the step that the unconfigured device uses the device information to decrypt the encrypted first access information can further include the following sub-steps.

[121] In sub-step S21, the unconfigured device uses the device information to generate a decryption key.

[122] In the embodiments of the present application, the unconfigured device uses the device information to generate the decryption key according to a specific key algorithm.

[123] The symmetric encryption algorithm requires that the decryption key is the same as the encryption key, the unconfigured device and the network hotspot device use the same key algorithm to generate the encryption key or the decryption key.

[124] In sub-step S22, the unconfigured device uses the decryption key to decrypt the encrypted first access information according to an inverse algorithm corresponding to the preset symmetric encryption algorithm.

[125] The decryption key of the unconfigured device is the same as the encryption key of the network hotspot device. During decryption, the unconfigured device uses an inverse algorithm corresponding to the symmetric encryption algorithm to decrypt the encrypted first access information.

[126] In the embodiments of the present application, when the user updates the access information of the Internet hotspot of the network hotspot device, causing the unconfigured device disconnected. The unconfigured device can be connected to the discovery hotspot of the network hotspot device. The network hotspot device judges whether the unconfigured device is in the preset white list. If the unconfigured device is in the white list, the network hotspot device accepts the device information sent by the unconfigured device through the discovery hotspot.

[127] The network hotspot device uses the device information to generate an encryption key, and then uses a symmetric encryption algorithm to encrypt the updated

access information of the Internet accessing hotspot, and then sends the encrypted access information to the unconfigured device.

[128] The unconfigured device uses its own device information to generate a decryption key, and then decrypts the encrypted access information according to the inverse algorithm corresponding to the symmetric encryption algorithm, and then uses the access information to access the Internet hotspot of the network hotspot device.

[129] The embodiments of the present application solves the problem of repeated network configuration of the device after the access information of the Internet hotspot being updated. The entire process is transparent to users, does not require user participation, and has an improved user experience. The entire process uses encryption measures to ensure data security, and uses device information for encryption, which can ensure the uniqueness of encryption for different devices and has a high security level.

[130] In order to enable those skilled in the art to better understand the embodiments of the present application, the following describes the embodiments of the present application through an example.

[131] Reference is given to **FIG. 4** which illustrates a flow chart of accessing a network hotspot device by a smart device of embodiments of the present application.

[132] The network hotspot device creates an Internet hotspot and a discovery hotspot after power-on.

[133] A user can configure the smart device through the user terminal, so that the smart device can access the hotspot of the network hotspot device.

[134] After the smart device is connected to the Internet hotspot, the network hotspot device adds the smart device to a white list.

[135] After the user updates the access information of the Internet hotspot, the network hotspot device disconnects the smart device from the Internet hotspot, causing the smart device to go offline.

[136] After the smart device goes offline, the smart device scans or attempts to connect to the Internet hotspot of the original network hotspot device. If the smart device fails to scan or connect to the Internet hotspot of the original network hotspot device, the smart device scans or attempts to connect to the discovery hotspot of the original network hotspot device.

[137] If the smart device successfully connects to the discovery hotspot of the network hotspot device, the network hotspot device evaluates the white list to determine whether the smart device is in the white list; if the smart device is in the white list, the network hotspot device queries the device information of the smart device.

[138] The smart device sends its own device information to the network hotspot device.

[139] The network hotspot device uses the device information to generate an encryption key. The network hotspot device uses the encryption key to encrypt the updated access information for the Internet hotspot according to a symmetric encryption algorithm, and then sends the encrypted access information to the smart device.

[140] The smart device uses the device information to generate the same decryption key as the encryption key. The smart device uses the decryption key, decrypts the access information according to the inverse algorithm corresponding to the symmetric encryption algorithm, and then uses the access information to connect to the Internet hotspot.

[141] It should be noted that, for simplicity of description, the method embodiments are expressed as a series of action combinations, but those skilled in the art

should know that the embodiments of the present application are not limited by the sequence of actions described, because according to the embodiments of the present application, some steps may be performed in other orders or simultaneously. Secondly, those skilled in the art should also know that the embodiments described in the specification are all preferred embodiments, and the involved actions are not necessarily required by the embodiments of the present application.

[142] Reference is given to **FIG. 5** which illustrates a structural diagram of embodiments of a system for accessing a network hotspot device by an unconfigured device of the present application, which specifically can include: a network hotspot device 501 and an unconfigured device 502.

[143] Network hotspot device 501 is used to create a first hotspot and a second hotspot; and after the first access information of the first hotspot is updated, network hotspot device 501 disconnects unconfigured device 502 that has accessed the first hotspot from network hotspot device 501.

[144] Unconfigured device 502 is used to access the second hotspot.

[145] Network hotspot device 501 is used to obtain the device information sent by unconfigured device 502 through the second hotspot, use the device information to encrypt the updated first access information, and send the encrypted first access information to unconfigured device 502.

[146] Unconfigured device 502 is also used to decrypt the encrypted first access information by using the device information and access the first hotspot by using the decrypted first access information.

[147] In the embodiments of the present application, network hotspot device 501 is also used to determine whether unconfigured device 502 is in the preset white list. If

unconfigured device 502 is in the preset white list, network hotspot device 501 accepts the device information sent by the unconfigured device 502.

[148] In the embodiments of the present application, network hotspot device 501 is also used to disconnect unconfigured device 502 from the second hotspot if unconfigured device 502 is not in the preset white list.

[149] In the embodiments of the present application, network hotspot device 501 is also used to generate an encryption key using the device information and encrypt the updated first access information using the encryption keys according to a preset symmetric encryption algorithm.

[150] In the embodiments of the present application, unconfigured device 502 is further used to generate a decryption key by using the device information and decrypting the encrypted first access information using the decryption keys according to an inverse algorithm corresponding to the preset symmetric encryption algorithm.

[151] In the embodiments of the present application, the system can further include a server.

[152] Network hotspot device 501 is also used to receive a preset white list sent by the server.

[153] In the embodiments of the present application, network hotspot device 501 is also used to add unconfigured device 502 to the preset whitelist after unconfigured device 502 accesses the first hotspot for the first time.

[154] In the embodiments of the present application, unconfigured device 502 is further configured to access the second hotspot using preset second access information for the second hotspot.

[155] For the device embodiment, since it is basically similar to the method embodiment, the description is relatively simple, and the relevant part can be referred to the description of the method embodiments.

[156] The embodiments of the present application also provide an apparatus, comprising:

[157] one or more processors; and

[158] one or more machine-readable media having stored thereon instructions that, when executed by the one or more processors, cause the apparatus to perform one or more of the methods described in the embodiments of the present application.

[159] The embodiments of the present application also provide one or more machine-readable medium having stored thereon instructions that, when executed by one or more processors, cause an apparatus to perform one or more of the methods described in the embodiments of the present application.

[160] The embodiments in this specification are described in a progressive manner. Each embodiment focuses on the differences from other embodiments, and the same or similar parts between the embodiments may refer to each other.

[161] Those skilled in the art should understand that the embodiments of the embodiments of the present application may be provided as methods, devices, or computer program products. Therefore, the embodiments of the present application may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware. Moreover, the embodiments of the present application may take the form of computer program products implemented on one or more computer usable storage media (including but not limited to disk storage, CD-ROM, optical storage, etc.) containing computer usable program code.

[162] The embodiments of the present application are described with reference to flowcharts and/or block diagrams of the method, terminal device (system), and computer program product according to the embodiments of the present application. It should be understood that each flow and/or block in the flowchart and/or block diagram and a combination of the flow and/or block in the flowchart and/or block diagram may be implemented by computer program instructions. These computer program instructions can be provided to the processor of a general-purpose computer, special-purpose computer, embedded processing machine, or other programmable data processing terminal device to produce a machine so that the instructions executed by the processor of the computer or other programmable data processing terminal device generate an apparatus for realizing functions specified in a block or blocks of a flowchart or a flow and/or a block diagram.

[163] These computer program instructions may also be stored in a computer readable memory that can guide a computer or other programmable data processing terminal device to work in a specific manner, so that the instructions stored in the computer readable memory produce an article of manufacture including an instruction device. The instruction device implements the functions specified in one block or multiple blocks of the flowchart one flow or multiple flows and/or block diagrams.

[164] These computer program instructions can also be loaded on a computer or other programmable data processing terminal device, so that a series of operation steps are performed on the computer or other programmable terminal device to generate computer-implemented processing, so that the instructions executed on the computer or other programmable terminal device provide steps for implementing functions specified in one block or multiple blocks of the flowchart one flow or multiple flows and/or block diagrams.

[165] Although the preferred embodiments of the embodiments of the present application have been described, those skilled in the art can make additional changes and modifications to these embodiments once they learn the basic inventive concept. Therefore, the appended claims are intended to be interpreted as including the preferred embodiments and all changes and modifications fall within the scope of the embodiments of the present application.

[166] Finally, it should also be noted that in this article, relational terms such as first and second are used only to distinguish one entity or operation from another entity or operation, and do not necessarily require or imply that there is any such actual relationship or order between entities and operations. Moreover, the terms "include", "include" or any other variant thereof are intended to cover non-exclusive inclusion, so that a process, method, article or terminal device that includes a series of elements includes not only those elements, but also those that are not explicitly listed, or also include elements inherent to such processes, methods, articles or terminal equipment. Without more restrictions, the element defined by the sentence "include one..." does not exclude that there are other identical elements in the process, method, article, or terminal device that includes the element.

[167] The above describes in detail a method for accessing a network hotspot device by an unconfigured device and a system for accessing a network hotspot device by an unconfigured device provided by this application, and a specific example is applied to the principle of the application in this article. The implementation examples are described. The descriptions of the above examples are only used to help understand the method and the core idea of the present application. At the same time, for those of ordinary skill in the art, according to the ideas of the present application, in the specific implementation manner

and application scope, all are subject to change. In summary, the content of this specification should not be interpreted as a limitation of this application.

WHAT IS CLAIMED IS:

1. A method for accessing a network hotspot device by an unconfigured device, characterized in that, the network hotspot device creates a first hotspot and a second hotspot, the method comprising:

after the first access information of the first hotspot been updated, disconnecting, by the network hotspot device, a connection between the unconfigured device that has accessed the network hotspot device through the first hotspot and the first hotspot of the network hotspot device;

accessing, by the unconfigured device, the second hotspot;

sending, by the network hotspot device, the updated first access information to the unconfigured device through the second hotspot; and

accessing, by the unconfigured device, the first hotspot using the first access information.

2. The method of claim 1, characterized in that, after sending, by the network hotspot device, the updated first access information to the unconfigured device through the second hotspot comprises:

receiving, by the network hotspot device, device information of the unconfigured device sent by the unconfigured device through the second hotspot;

encrypting, by the network hotspot device, the updated first access information with the device information and sending the encrypted first access information to the unconfigured device.

3. The method of claim 2, characterized in that, the step of accessing, by the unconfigured device, the first hotspot using the first access information comprises:

decrypting, by the unconfigured device, the encrypted first access information using the device information and accessing the first hotspot using the decrypted first access information.

4. The method of claim 2, characterized in that, the step of receiving, by the network hotspot device, the device information of the unconfigured device sent by the unconfigured device through the second hotspot comprises:

determining, by the network hotspot device, whether the unconfigured device is in a preset white list; and

if the unconfigured device being in the preset white list, accepting, by the network hotspot device, the device information sent by the unconfigured device.

5. The method of claim 4, characterized in, further comprising:

if the unconfigured device not being in the preset white list, disconnecting, by the network hotspot device, a connection between the unconfigured device and the second hotspot.

6. The method of claim 3, characterized in that, the step of encrypting, by the network hotspot device, the updated first access information with the device information comprises:

generating, by the network hotspot device, an encryption key using the device information; and

encrypting, by the network hotspot device, the updated first access information using the encryption key according to a preset symmetric encryption algorithm.

7. The method of claim 6, characterized in that, the step of decrypting, by the unconfigured device, the encrypted first access information using the device information comprises:

generating, by the unconfigured device, a decryption key using the device information;

decrypting, by the unconfigured device, the encrypted first access information using the decryption key according to an inverse algorithm corresponding to the symmetric encryption algorithm.

8. The method of claim 4, characterized in, further comprising:

receiving, by the network hotspot device, the preset white list from a server.

9. The method of claim 4, characterized in, further comprising:

after the unconfigured device accessing to the first hotspot at the first time, adding, by the network hotspot device, the unconfigured device to the preset white list.

10. The method of claim 1, characterized in that, the step of accessing, by the unconfigured device, the second hotspot comprises:

accessing, by the unconfigured device, the second hotspot using preset second access information for the second hotspot.

11. A system for accessing a network hotspot device by an unconfigured device, characterized in, comprising: a unconfigured device and a network hotspot device, wherein the network hotspot device is used to create a first hotspot and a second hotspot and to disconnect a connection between the unconfigured device that has accessed the network

hotspot device through the first hotspot and the first hotspot of the network hotspot device after first access information of the first hotspot having been updated,

the unconfigured device is used to access the second hotspot,

the network hotspot device is used to send the updated first access information to the unconfigured device through the second hotspot, and

the unconfigured device is used to access the first hotspot using the first access information.

12. The system of claim 11, characterized in:

the network hotspot device is further used to receive device information of the unconfigured device sent by the unconfigured device through the second hotspot, to encrypt the updated first access information with the device information, and to send the encrypted first access information to the unconfigured device.

13. The system of claim 12, characterized in that,

the unconfigured device is further used to decrypt the encrypted first access information using the device information and to access the first hotspot using the decrypted first access information.

14. The system of claim 12, characterized in that:

the network hotspot device is used to determine whether the unconfigured device is in a preset white list and to accept the device information sent by the unconfigured device if the unconfigured device is in the preset white list.

15. The system of claim 14, characterized in that:

the network hotspot device is further used to disconnect a connection between the unconfigured device and the second hotspot if the unconfigured device is not in the preset white list.

16. The system of claim 13, characterized in that:

the network hotspot device is further used to generate an encryption key using the device information and to encrypt the updated first access information using the encryption key according to a preset symmetric encryption algorithm.

17. The system of claim 16, characterized in that:

the unconfigured device is further used to generate a decryption key using the device information and decrypt the encrypted first access information using the decryption key according to an inverse algorithm corresponding to the symmetric encryption algorithm.

18. The system of claim 14, characterized in, further comprising a server:

the network hotspot device is further used to receive the preset white list from a server.

19. The apparatus of claim 14, characterized in that:

the network hotspot device is further used to add the unconfigured device to the preset white list after the unconfigured device accesses to the first hotspot at the first time.

20. The system of claim 11, characterized in that:

the unconfigured device is further used to access the second hotspot using preset second access information for the second hotspot.

21. An apparatus for accessing a network hotspot device by an unconfigured device, characterized in, comprising:

one or more processors; and

one or more machine-readable media having stored thereon instructions that, when executed by the one or more processors, cause the apparatus to perform one or more of the methods described in claims 1-10.

22. One or more machine-readable medium having stored thereon instructions that, when executed by one or more processors, cause an apparatus to perform one or more of the methods described in claims 1-10.