

ONE-TIME WIRELESS AUTHENTICATION OF AN INTERNET-OF-THINGS DEVICE

BACKGROUND

[001] Today, the use of Internet-of Things (IoT) devices are proliferating. An IoT device is an electronic computing device that connects wirelessly to a network and has the ability to transmit data over the network. IoT devices are nonstandard computing devices in that they are typically not equipped with a user interface for user interaction and focus instead on machine-to-machine communication. The lack of a user interface can be problematic when the IoT device needs to connect to the wireless network the first time with necessary access credentials (e.g., user name and password), which are typically entered by a user. If the IoT has the requisite size, then the IoT device can be equipped with some type of user interface, such as a small keyboard and/or screen. However, adding a user interface comes at a cost.

[002] Accordingly, it be desirable to provide an improved method and system for wireless authentication of an IoT device.

BRIEF SUMMARY

[003] The exemplary embodiments provide methods and systems for one-time wireless authentication of an Internet-of-Things device. Aspects of exemplary embodiment include receiving, by a proxy application executing on a mobile device during a registration process, a device ID associated with the IoT device. The proxy application transmits the device ID to a router of the wireless network. Subsequent to the registration process, the proxy application receives the device ID from the router in response to the router receiving an authorization request with no network password from the IoT device

for access to the wireless network, where the router forwards the device ID to the proxy application. The proxy application prompts the user of the mobile device to enter the password, and transmits the entered network password to the router, such that the router validates the password and grants the IoT device access to the wireless network, the IoT device transmits the IoT device ID to the router for subsequent network connection without a need for the mobile device.

[004] In another embodiment, methods and systems for one-time wireless authentication of an Internet-of-Things device comprises a router receiving a registration request from a proxy application executing on a mobile device, the registration request including a device identifier associated with the IoT device, the device identifier entered into the proxy application by a user of the mobile device, the router further storing the device identifier and enabling a proxy authentication setting. The router receives an authorization request from the IoT device for access to a wireless network, the authorization request comprising at least the device identifier without a network password. The router determines if a proxy authentication setting is enabled, and if so forwards the device identifier to the proxy application. The router receives a message from the proxy application, a message including a network password entered into the proxy application by the user. Responsive to the router validating the network password, the router grants the IoT device access to the wireless network, wherein the IoT device transmits the device identifier to the router for subsequent connection without a need for the mobile device or the proxy application.

[005] According to the method and system disclosed herein, the disclosed embodiments enable easy wireless Internet conductivity for an Internet-of-Things device

having no provisions for password entry, thus eliminating the need for keys and user interaction through the Internet-of-Things device. The methods and systems facilitate such Internet-of-Things devices to connect to the Internet of long as the Internet-of-Things devices are pre-configured for proxy authentication using the mobile application in conjunction with software changes in the router.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[006] Figure 1 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a first embodiment.

[007] Figure 2 is a flow diagram illustrating an overview of a process for one-time wireless authentication of an Internet-of-Things device in accordance with some embodiments.

[008] Figure 3 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a second embodiment.

[009] Figure 4 is a flow diagram illustrating the process for one-time wireless authentication of an Internet-of-Things device in accordance with the second embodiment of Figure 3.

[010] Figure 5 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a third embodiment.

[011] Figure 6 is a flow diagram illustrating the process for one-time wireless authentication of an Internet-of-Things device in accordance with the third embodiment of Figure 3.

[012] Figure 7 shows an implementation of a computer system that may be applicable to IoT device, the mobile device, the authentication mapping server and/or the router mapper system.

DETAILED DESCRIPTION

[013] The exemplary embodiment relates to a mobile application for one-time wireless authentication of an Internet-of-Things device. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the exemplary embodiments and the generic principles and features described herein will be readily apparent. The exemplary embodiments are mainly described in terms of particular methods and systems provided in particular implementations. However, the methods and systems will operate effectively in other implementations. Phrases such as "exemplary embodiment", "one embodiment" and "another embodiment" may refer to the same or different embodiments. The embodiments will be described with respect to systems and/or devices having certain components. However, the systems and/or devices may include more or less components than those shown, and variations in the arrangement and type of the components may be made without departing from the scope of the invention. The exemplary embodiments will also be described in the context of particular methods having certain steps. However, the method and system operate effectively for other methods having different and/or additional steps and steps in different

orders that are not inconsistent with the exemplary embodiments. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features described herein. As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or send (e.g., transmit) information to the other unit. This may refer to a direct or indirect connection that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively send information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and sends the processed information to the second unit. In some non-limiting embodiments, a request or message may refer to a network packet (e.g., a data packet and/or the like) that includes data.

[014] To provide context for the disclosed embodiments, today a wireless router provides and communications over a local or home wireless (Wi-Fi) network and connects to the Internet via a modem. An electronic device needing access to the wireless network

needs to send access credentials, such as a network password, to the router. The first time an electronic device connects to the wireless network, a user typically inputs the network password, which is transmitted to the router. The router then sends an authentication request with the access credentials to a credential management system. The credential management system can be local to the router or a remote server. The credential management system receives the authentication request and authenticates the access credentials against previously stored access credentials for the router. The credential management system sends a response to the router either allowing or denying network access, and the router then either grants the device network access or alternatively sends a denial message.

[015] For electronic devices with no provisions for manual entry of access credentials, such as an Internet-of-Things (IoT) device, methods and systems are required to facilitate easy wireless network and Internet connectivity through the router.

[016] According to the disclosed embodiments, a one-time authentication process is provided for an IoT device to use a wireless network without the need for the IoT device to have a user interface for entering access credentials. Instead, a mobile phone of the user, and in particular, an application on the mobile phone, acts as a proxy to provide one-time wireless authentication of the IoT device with a router of a wireless network during first access. Thereafter, if the IoT device becomes disconnected from the network, the IoT device can reconnect to the network by transmitting the device ID of the IoT device to the router for subsequent connection without requiring aid of the mobile device. Several

embodiments are herein described that collectively unify the idea of proxy authentication by encapsulating underlying security controls and data distribution.

[017] Figure 1 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a first embodiment. The system 10 includes a router 12 that provides a network 14 and communicates over the network 14 and the Internet 20. The router 12 is connected to the Internet 20 through a gateway (not shown). In one embodiment, the network is a wireless network, but wired connections (e.g., Ethernet) with the router 12 can also be made. As used herein, a “router” is a networking device forwards data packets between computer networks for example, in the home and small office environment, Internet protocol (IP) routers simply forward IP packets between home/office computing devices and the Internet.

[018] A mobile device 16 is wirelessly connected to the network 14, and an Internet-of-Things (IoT) device 18 requires first time access to the network 14. A “mobile device” may be a device that is operated by a user. Examples of mobile devices 16 may include a mobile phone, a smart phone, a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a thin-client device, a tablet PC, etc. Additionally, mobile devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The mobile device 16 may include one or more processors capable of processing user input. The mobile device 16 may also include one or more input sensors for receiving user input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones,

etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The mobile device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G, 5G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

[019] As used herein, an Internet of things (IoT) device describes an electronic device—“a thing”—that is embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet or other network.

[020] The router 12 may communicate with a credential management system 22, which maintains an access credentials database 24. When the router 12 receives an authentication request from a device, e.g., the IoT device 18, for network access, the router 12 may forward the authentication request to the credential management system 22 to authenticate the requesting device.

[021] The IoT device 18 is associated with a device identifier (ID) 34, and the proxy application 24 is associated with an application (app) ID 32. The IDs 34 and 32 may include any distinctive set of alphanumeric characters (numbers, graphics, symbols letters or other information) that can be used to identify a device or a program. For

example, the device ID 34 may comprise a serial number, partial serial number, a key and the like, or a combination thereof, associated with the IoT device 18.

[022] In one embodiment, the router 12, the IoT device 18, and the mobile device 18 are configured to receive and transmit messages over the network 14 using the Internet protocol suite otherwise known as Transmission Control Protocol (TCP) and the Internet Protocol (IP) or TCP/IP.

[023] According to the disclosed embodiments, since a user cannot enter the access credentials for the network 14 on the IoT device 18 due its lack of a user interface, the system 10 further includes a mobile application, referred to herein as a proxy application (proxy app) 24 that acts a proxy for the IoT device 18 during the first network authentication attempt with the router 12, and a proxy authentication setting 28 for the router 12. In embodiments, the authentication mapping server 26 maintains a mapping between the IoT device 18 and the proxy application 24.

[024] According to embodiments, the system 10 associates the proxy app 24 with the app ID 32. The app ID 32 may be a special purpose software key, a mobile phone number associated with the mobile device 16, a partial phone number, a software key, and the like, or a combination thereof. When associated with the proxy application 24, the app ID 32 may be used by the system 10 to determine the mobile device 16 on which the proxy application 24 is installed.

[025] Figure 2 is a flow diagram illustrating an overview of a process for one-time wireless authentication of an Internet-of-Things device in accordance with some embodiments. As an overview, the process occurs between the router 12 and the proxy

application 24 executing on the mobile device 16 of the user. The process assumes that access credentials, such as a password, for the wireless network 14 have been sent from the router 12 to the credential management system 22 and stored in access credentials database 24. The process further assumes the user has installed the proxy application 24 on the user's mobile device 16 in order to configure the IoT device 18 for a one-time proxy authentication to the wireless network 14.

[026] The one-time wireless authentication process includes a registration phase in which the proxy application 24 is opened and receives the device ID 34 associated with the IoT device 18 that is entered by a user (block 200). This step may be initiated in response to a user who wants to set up the IoT device 18 and presses a "registration button" displayed by proxy application 24 to register the IoT device 18. Thereafter, the proxy application 24 displays a field into which the user may enter the device ID 34. The device ID 34 may comprise a serial number or other identifier of the IoT device 18. The user may find the device ID 34 on the IoT device 18 itself or in documentation provided with the IoT device 18.

[027] The proxy application 24 transmits the device ID to the router 12 in a registration request (block 201). The router 12 receives the registration request, stores the device ID 34 in the credential management system 22, and enables the proxy authentication setting 28 (block 202). In one embodiment, the credential management system 22 may comprise part of a local backend system for the router 12. In another embodiment, the credential management system 22 may be a remote site on the Internet

20. The proxy authentication setting can be stored by the router 12 or by the credential management system 22.

[028] In one embodiment, the registration phase may include the proxy application 24 associating the device ID 34 with the app ID 32 of the proxy application 24. In one embodiment, a mapping of the device ID 34 to the app ID 32 may be registered as an ID pair with the router 12 or another system (e.g., an authentication mapper server 326 shown in Figure 3). In one embodiment, the proxy application 24 sends both the device ID 34 the app ID 32 as an ID pair in the registration request sent to the router 12 in block 201. The router 12 may then store the mapping of the ID pair in the credential management system 22 or forward the ID pair to another system in block 202.

[029] Subsequent to the registration process, the router 12 receives, an authorization request from the IoT device 18 over the network 14, wherein the authorization request comprises at least the device ID 34 without a network password (block 204). In one embodiment, when the IoT device 18 is first turned on, the IoT device 18 may be configured to determine automatically which one of a plurality of detected wireless networks to request access. This may be done by selecting the network 14 having the highest signal strength based on the assumption that the physically closest router 12 would have the best signal, as is typically the case in a local network environment. If the IoT device 18 fails to receive a reply to the authorization request within a predetermined time threshold, the IoT device 18 may send an authentication request to a router of another network having the next highest signal strength and so on until the IoT device finds the router with proxy authentication enabled.

[030] The router 12 then determines if the proxy authentication setting 28 is enabled, and if so, forwards the device ID 34 to the proxy application 24 (block 206). If the proxy authentication setting 28 is not enabled, the process ends with the router sending a denial message to the IoT device 18. The proxy application 24 receives the device ID 34 from the router 12, and optionally validates the device ID (block 208). In response to the proxy application 24 validating the device ID 34 (e.g., by checking an internal setting, table or database), the proxy application 24 prompts the user to enter the network password and receives the entered network password (block 210). The proxy application 24 then transmits the entered network password in a message to the router 12 (block 212).

[031] The router 12 receives a message including the entered network password and validates the entered network password (block 214). In one embodiment, the router 12 validates the entered network password by sending a validation request to the credential management system 22, which validates the network password if a match is found for the password in the access credentials database 24. In one embodiment, the credential management system 22 may be part of a backend system for the router.

[032] Responsive to validating the entered network password, the router 12 sends a success message to the IoT device 18 granting access to the wireless network, wherein the IoT device 18 transmits the device ID 34 to the router 12 for subsequent connection without a need for the network password, the mobile device 16, or the proxy application 24 (block 216). That is, the IoT device 18 typically stays connected to the wireless network 14, but if the IoT device 18 becomes disconnected, the IoT device 18 resends the device

ID 34 to the router 12. The router 12 looks up the device ID 34 and if found reestablishes the network connection, all without any input from the user or the mobile device 16.

[033] Figure 3 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a second embodiment, where like components from Figure 1 have like reference numerals.

[034] The system 300 is similar to the system 10 of Figure 1, except provides additional security by separating functionality of the proxy application into two separate applications (apps), referred to herein as proxy app A 324A and proxy app B 324B, installed on mobile device 16. In this embodiment, proxy app A 324A is associated with an app A ID 32A and proxy app B 324B is associated with an app B ID 32B. Both the app A ID 32A and the app B ID 32B may include the unique mobile phone number of the mobile device 16 in which the apps are installed.

[035] According to one embodiment, for additional security the proxy system 300 further includes an authentication mapper server 326 in communication with the router 312 over the Internet 20, which is configured to communicate request and responses for proxy app A 324A and proxy app B 324B so that proxy app A 324A and proxy app B 324B do not communicate with one another directly. The term “server” may refer to one or more computing devices, such as processors, storage devices, and/or similar computer components, that communicate with client devices and/or other computing devices over a network, such as the Internet or private networks and, in some examples, facilitate communication among other servers and/or client devices. For example, the server

computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server, and may include or be coupled to a database.

[036] In one embodiment, the authentication mapper server 326 communicate with proxy app A 324A and proxy app B 324B though, for example, a Representational state transfer (REST) application programming interface (API) or REST API.

[037] This second embodiment provides additional security by establishing distributed controls and distributed ownership on the data. For example, the authentication mapper server 326 may have control over network authentication and may be provided and/or run by a manufacturer of the router 312. Any subsequent need of decoupling or disabling a IoT device 18 from proxy authentication may require the manufacturer of the IoT device 18 to update the authentication mapper server 326 through the router manufacture.

[038] In one embodiment, proxy app A 324A is configured to receive from the router 312 the device ID 34 of the IoT device 18 during the request for network authorization, and determine if that specific IoT device has been enabled for proxy authentication by forwarding the device ID 34 to the authentication mapper server 326 to validate the device ID. Proxy app B 324B is configured to respond to a validation message from the authentication mapper server 326 by displaying a popup screen prompting the user to enter the network password and to send the entered network password to the router 512 for validation through the authentication mapper server 326 and proxy app A 324A, as explained below.

[039] Technically proxy app A 324A and proxy app B 324B have different functionalities, but in an alternative embodiment can be combined into one proxy application on the mobile device 16, as in Figure 1. Also multiple IoT devices can use the dual proxy applications or the single proxy application in the mobile device 16 for this initial setup.

[040] Figure 4 is a flow diagram illustrating the process for one-time wireless authentication of an Internet-of-Things device in accordance with the second embodiment of Figure 3. The one-time wireless authentication process includes a registration phase that assumes once proxy app A 324A and proxy app B 324B are started the first time on the mobile device 16, proxy app A 324A and proxy app B 324B register the respective app A ID 32A and the app B ID 32B as an application pair with the authentication mapper server 326. The authentication mapping server 326 may store the registration of the app A ID 32A and the app B ID 32B as an application ID pair in the mapping database 302.

[041] Referring both to Figures 3 and 4, during the registration phase proxy app A 324A displays a user interface in which to receive the device ID 34 associated with the IoT device 18 entered by a user (block 400). This step may be initiated in response to a user desiring to set up the IoT device 18 and pressing a “registration button” on proxy app A 324A or proxy app B 324B to register the IoT device 18. Thereafter, the proxy app A 324A displays a field into which the user may enter the device ID 34. Proxy app A 324A receives the device ID 34 and transmits both the app A ID 32A and device ID 34 as an ID pair in a registration request to the router 312 (block 401).

[042] The router 312 receives the registration request, i) enables the proxy authentication setting 28, ii) stores at least the device ID 34, and iii) forwards the ID pair

to the authentication mapper server 326 in a registration request (block 402). Once the authentication mapper server 326 receives the ID pair, the authentication mapper server 326 uses the app A ID 32A to find the record 304 having a matching app A ID 32A in the mapping database 302, and stores/associates the device ID 34 with the application ID pair in record 304. In an alternative embodiment, proxy app B 324B may be used instead of proxy app A 324A in the above registration process.

[043] Subsequent to the registration process, the router 312 receives, an authorization request from the IoT device 18 over the network 14, wherein the authorization request comprises at least the device ID 34 without a network password (block 404). As an example, the authorization request may include DeviceID: “tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678” for instance.

[044] The router 312 then determines if the proxy authentication setting 28 is enabled, and if so, forwards the device ID 34 to the proxy app A 324A (block 406). In one embodiment, the router 312 receives and forwards the authorization request over the network 14 using the Internet protocol suite otherwise known as Transmission Control Protocol (TCP) and the Internet Protocol (IP).

[045] Proxy app A 324A receives the device ID 34 from the router 312, and forwards the device ID 34 in a validation request to the authentication mapper server 326 for validation (block 408). In response, proxy app B 324B receives a validation response from the authentication mapper server 326 in response to the validation request of proxy app A 324A (block 410A). In embodiments, the authentication mapper server 326 upon receiving the validation request, first uses the device ID 34 to search the mapping

database 302 to find the mapping record 304 having a matching device ID 34, and once found, the authentication mapper server 326 sends the validation response to the proxy app B 324B listed in the matching mapping record 304 via the preconfigured REST API.

[046] For example the authentication mapper server 326 may store the preconfigured REST API as:

(https://www.appa.appid/{info}) APP A –
deviceKey:"tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678----→ APP B
(https://www.appb.appld/{Info}),

where the preconfigured REST API informs the authentication mapper server 326 to call https://www.appb.appld/{Info} registered by app B, for any incoming requests from App A corresponding to deviceKey:"tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678.

[047] In response to receiving the response from the authentication mapper server 326 validating the device ID 34, proxy app B 324B prompts the user to enter the network password and receives the entered network password (block 410B). Proxy app B 324B then transmits the entered network password in a message to the authentication mapper server 326 for forwarding to proxy app A 324A via the preconfigured REST API (block 412A). Proxy app A 324A then transmits the entered network password in a message to the router 12 (block 412B).

[048] The router 312 receives a message including the entered network password and validates the entered network password (block 414). In one embodiment, the router 312 validates the entered network password by sending a validation request to the credential management system 22, which does so if a match is found for the password in

the access credentials database 24. In one embodiment, the credential management system 22 may be part of a backend system for the router 312.

[049] Responsive to validating the entered network password, the router 312 sends a success message to the IoT device 18 granting access to the wireless network, wherein the IoT device 18 transmits the device ID 34 to the router 312 for subsequent connection without a need for the network password, the mobile device 16 or the proxy applications 324A and 324B (block 416).

[050] Figure 5 is a block diagram illustrating a system for enabling a mobile application to provide one-time wireless authentication of an Internet-of-Things device according to a third embodiment, where like components from Figure 3 have like reference numerals. The system 500 is similar to the system 300 of Figure 3, except in addition to using the two separate proxy applications, proxy app A 324A and proxy app B 324B, system 500 further includes a router mapper system 502. In this embodiment, proxy app A 324A is associated with an app A ID 32A and proxy app B 324B is associated with an app B ID 32B, where both the app A ID 32A and the app B ID 32B may include the unique mobile phone number of the mobile device 16 in which the apps are installed.

[051] The third embodiment enables the manufacturer of the router 512 and the manufacturer of the IoT device 18 to share responsibility for the proxy authentication. For example, the manufacturer of the router 512 may control the router mapper system 504, while the manufacturer of the IoT device 18 may control the authentication mapper server 326. During the proxy authentication process, input from both the router mapper system

504 and the authentication mapper server 326 is required, as described with respect to Figure 6.

[052] Figure 6 is a flow diagram illustrating the process for one-time wireless authentication of an Internet-of-Things device in accordance with the third embodiment of Figure 5. The one-time wireless authentication process includes a registration phase that assumes once proxy app A 324A and proxy app B 324B are started the first time on the mobile device 16 that: i) a mapping between the app A ID 32A and the network password (PW) is registered with the router mapper system 504; and ii) the app B ID 32B is registered with the authentication mapper server 326. This pre-mapping process safeguards the router 512 from having to receive authentication request from proxy apps on connected mobile devices other than from authorized proxy app A 324A and proxy app B 324B on mobile device 16 by checking any such request against the router DB 506 and the mapping DB 302.

[053] Referring both to Figures 5 and 6, during the registration phase proxy app A 324A displays a user interface in which to receive the device ID 34 associated with the IoT device 18 entered by a user (block 600). Proxy app A 324A receives the device ID 34 and transmits both the app A ID 32A and device ID 34 as an ID pair in a registration request to the router 312 (block 601).

[054] The router 312 upon receiving the registration request: i) enables the proxy authentication setting 28, ii) stores at least the device ID 34, and iii) forwards the device ID pair to the router mapper system 504 in one registration request, and iv) forwards the

app B ID 32B and the device ID 34 to the authentication mapper server 326 in another registration request (block 602).

[055] As shown in Figure 5, the router mapper system 504 may store the device ID 34 in a record 508 of router database 506 associating app A ID 32A and the network password. Similarly, the authentication mapper server 326 may store the device ID 34 in a record 304 of mapping database 302 containing the app B ID 32B.

[056] Subsequent to the registration process, the router 312 receives an authorization request from the IoT device 18 over the network 14, wherein the authorization request comprises at least the device ID 34 without a network password (block 604). As an example, the authorization request may include DeviceID: "tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678" for instance.

[057] The router 312 then determines if the proxy authentication setting 28 is enabled, and if so, forwards the device ID 34 to the router mapper system 504 (block 606).

[058] The router mapper system 504 receives the device ID 34 and uses the device ID 34 to find, and send a notification message to, the proxy app A 324A mapped to the device ID 34 by the app A ID 32A (block 608). In one embodiment, the notification message is sent using the preconfigured REST API. For example the router mapper system 504 may store the preconfigured REST API as:

(https://www.appa.appid/{info}) APP A –
deviceKey:"tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678"----→ Mobile
device

APP A (<https://www.appa.appld/{Info}>),

where the preconfigured REST API in the router mapper system 504 informs the authentication mapper server 326 to call <https://www.appa.appld/{Info}> registered by app A, for any incoming requests from the router 512 corresponding to deviceKey: "tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678.

[059] In response, proxy app A 324A receives the notification message from the router mapper system 504 and forwards the notification message through the router-Internet to the authentication mapper server 326 (block 610). In response, proxy app B 324B receives a validation response from the authentication mapper server 326 in response to notification message from proxy app A 324A (block 612). That is, the authentication mapper server 326 first uses the device ID 34 received from proxy app A 324A to search the mapping database 302 to find the mapping record 304 having a matching device ID, and once the matching mapping record 304 is found, the authentication mapper server 326 sends the validation response to the proxy app B 324B mapped to the device ID in mapping record 304 via the preconfigured REST API.

[060] For example the authentication mapper server 326 may store the preconfigured REST API as:

(<https://www.appa.appld/{info}>) APP A –
deviceKey:"tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678----→ APP B
(<https://www.appb.appld/{Info}>),

where the preconfigured REST API informs the authentication mapper server 326 to call <https://www.appb.appld/{Info}> registered by app B, for any incoming requests from App A corresponding to deviceKey:"tdrgsthawu2n4n5j9aj4l5n2v97cm3bc78h3vn678.

[061] In response to receiving the response from the authentication mapper server 326 validating the device ID 34, the proxy app B 324B prompts the user to enter the network password and receives the entered network password (block 614). Proxy app B 324B then transmits the entered network password in a message to the authentication mapper server 326 for forwarding to proxy app A 324A via the preconfigured REST API (block 616). Proxy app A 324A then transmits the entered network password in a message to the router mapper system 504 using the REST API (block 618).

[062] The router mapper system 504 receives a message including the entered network password and upon finding a matching network password, transmits the network password to the router 512 (block 620). The router 512 receives a message including the entered network password and validates the network password (block 622). In one embodiment, the router 512 validates the entered network password by sending a validation request to the credential management system 22, which does so if a match is found for the password in the access credentials database 24.

[063] Responsive to validating the entered network password, the router 512 sends a success message to the IoT device 18 granting access to the wireless network, wherein the IoT device 18 transmits the IoT device ID to the router 512 for subsequent connection without a need for the network password, the mobile device 16 or the proxy applications 324A and 324B (block 624).

[064] Methods and systems for one-time wireless authentication of an IoT device have been described. Methods and systems facilitate easy wireless Internet conductivity for an IoT device when there is no available means for manual entry of passwords from

the IoT device, thus eliminating the need for keys and user interaction through the IoT device 18. The methods and systems facilitate IoT devices having no provisions for password entry to connect to the Internet of long as the IoT devices are pre-configured for proxy authentication using one or more mobile application and in addition to software changes in the router.

[065] Figure 7 shows an implementation of a computer system 700 that may be applicable to IoT device 18, the mobile device 16, the authentication mapping server 26 and/or the router mapper system 504. According to an embodiment. The computer system 700 can include a microprocessor(s) 703 and memory 702. In an embodiment, the microprocessor(s) 703 and memory 702 can be connected by an interconnect 701 (e.g., bus and system core logic). In addition, the microprocessor 703 can be coupled to cache memory 709. In an embodiment, the interconnect 701 can connect the microprocessor(s) 703 and the memory 702 to input/output (I/O) device(s) 705 via I/O controller(s) 707. I/O devices 705 can include a display device and/or peripheral devices, such as mice, keyboards, modems, network interfaces, printers, scanners, video cameras and other devices known in the art. In an embodiment, (e.g., when the data processing system is a server system) some of the I/O devices (705), such as printers, scanners, mice, and/or keyboards, can be optional.

[066] In an embodiment, the interconnect 701 can include one or more buses connected to one another through various bridges, controllers and/or adapters. In one embodiment, the I/O controllers 707 can include a USB (Universal Serial Bus) adapter for

controlling USB peripherals, and/or an IEEE-1394 bus adapter for controlling IEEE-1394 peripherals.

[067] In an embodiment, the memory 702 can include one or more of: ROM (Read Only Memory), volatile RAM (Random Access Memory), and non-volatile memory, such as hard drive, flash memory, etc. Volatile RAM is typically implemented as dynamic RAM (DRAM) which requires power continually in order to refresh or maintain the data in the memory. Non-volatile memory is typically a magnetic hard drive, a magnetic optical drive, an optical drive (e.g., a DV D RAM), or other type of memory system which maintains data even after power is removed from the system. The non-volatile memory may also be a random access memory.

[068] The non-volatile memory can be a local device coupled directly to the rest of the components in the data processing system. A non-volatile memory that is remote from the system, such as a network storage device coupled to the data processing system through a network interface such as a modem or Ethernet interface, can also be used.

[069] In this description, some functions and operations are described as being performed by or caused by software code to simplify description. However, such expressions are also used to specify that the functions result from execution of the code/instructions by a processor, such as a microprocessor.

[070] Alternatively, or in combination, the functions and operations as described here can be implemented using special purpose circuitry, with or without software instructions, such as using Application-Specific Integrated Circuit (ASIC) or Field-Programmable Gate Array (FPGA). Embodiments can be implemented using hardwired circuitry without

software instructions, or in combination with software instructions. Thus, the techniques are limited neither to any specific combination of hardware circuitry and software, nor to any particular source for the instructions executed by the data processing system.

[071] While one embodiment can be implemented in fully functioning computers and computer systems, various embodiments are capable of being distributed as a computing product in a variety of forms and are capable of being applied regardless of the particular type of machine or computer-readable media used to actually effect the distribution.

[072] At least some aspects disclosed can be embodied, at least in part, in software. That is, the techniques may be carried out in a computer system or other data processing system in response to its processor, such as a microprocessor, executing sequences of instructions contained in a memory, such as ROM, volatile RAM, non-volatile memory, cache or a remote storage device.

[073] Routines executed to implement the embodiments may be implemented as part of an operating system or a specific application, component, program, object, module or sequence of instructions referred to as "computer programs." The computer programs typically include one or more instructions set at various times in various memory and storage devices in a computer, and that, when read and executed by one or more processors in a computer, cause the computer to perform operations necessary to execute elements involving the various aspects.

[074] Although specific embodiments have been described above, these embodiments are not intended to limit the scope of the present disclosure, even where only a single embodiment is described with respect to a particular feature. Examples of

features provided in the disclosure are intended to be illustrative rather than restrictive unless stated otherwise. The above description is intended to cover such alternatives, modifications, and equivalents as would be apparent to a person skilled in the art having the benefit of the present disclosure.

[075] Methods and systems for one-time wireless authentication of an Internet-of-Things device has been disclosed. The present invention has been described in accordance with the embodiments shown, and there could be variations to the embodiments, and any variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

CLAIMS

We Claim:

1. A computer-implemented method for authentication of an Internet-of-Things (IoT) device, comprising:

receiving, by a proxy application executing on a mobile device during a registration process, a device identifier associated with the IoT device, the device identifier entered into the proxy application by a user of the mobile device;

transmitting, by the proxy application, the device identifier to a router of a wireless network as part of the registration process;

subsequent to the registration process, receiving by the proxy application, the device identifier from the router in response to the router receiving an authorization request comprising the device identifier with no network password from the IoT device for access to the wireless network, and the router forwarding the device identifier to the proxy application after determining that the router has proxy authentication enabled;

prompting the user of the mobile device to enter the network password, and transmitting the entered network password in a message to the router, such that in response to the router validating the network password and granting the IoT device access to the wireless network, the IoT device transmits the device identifier to the router for subsequent network connection without a need for the mobile device or the proxy application.

2. The method of claim 1, wherein the registration phase further comprises: associating, by the proxy application, the device identifier with an application identifier used to identify the proxy application.
3. The computer-implemented method of claim 2, wherein the registration phase further comprises: registering, by the proxy application, a mapping of the device identifier to the application identifier as an identifier pair with the router.
4. The computer-implemented method of claim 3, wherein the registration phase further comprises: sending, by the proxy application, the identifier pair to the router such that the router stores the identifier pair in a credential management system or forwards the identifier pair to an authentication mapper server.
5. The computer-implemented method of claim 2, further comprising: separating functionality of the proxy application into a first proxy application and a second proxy application, wherein during the registration phase, the first proxy application and the second proxy application register as an application pair with an authentication mapper server.
6. The computer-implemented method of claim 5, further comprising: configuring the authentication mapper server to communicate request and responses for the first proxy application and the second proxy application.
7. The computer-implemented method of claim 6, further comprising: configuring the first proxy application to receive from the router the device identifier of the IoT device and

determine if the IoT device has been enabled for proxy authentication by forwarding the device identifier to the authentication mapper server to validate the device identifier.

8. The computer-implemented method of claim 6, further comprising: configuring the second proxy application to prompt the user of the mobile device to enter the network password in response to receiving a validation message from the authentication mapper server, and transmit the entered network password in the message to the router through the authentication mapper server and the first proxy application.

9. The computer-implemented method of claim 1, further comprising: implementing the proxy application as a first proxy application associated with a first application identifier and a second proxy application associated with a second application identifier, wherein the first application identifier and the second application identifier include a mobile phone number of the mobile device.

10. The computer-implemented method of claim 9, further comprising:
registering a mapping between the first application identifier and the network password with a router mapper system; and
registering the second application identifier with an authentication mapper server.

11. The computer-implemented method of claim 1, wherein receiving, by the proxy application, the device identifier associated with the IoT device further comprises: automatically determining, by the IoT device, which one of a plurality of detected wireless networks to request access to by selecting the wireless network having a highest signal strength.

12. A computer-implemented method for authentication of an IoT device, comprising:
receiving, by a router, a registration request from a proxy application executing on a mobile device, the registration request including a device identifier associated with the IoT device, the device identifier entered into the proxy application by a user of the mobile device, the router further storing the device identifier and enabling a proxy authentication setting;

receiving, by the router, an authorization request from the IoT device for access to a wireless network, the authorization request comprising at least the device identifier without a network password;

determining, by the router, if a proxy authentication setting is enabled, and if so forwarding the device identifier to the proxy application;

receiving, by the router, a message from the proxy application, a message including a network password entered into the proxy application by the user; and

responsive to the router validating the network password, granting the IoT device access to the wireless network, the IoT device to transmit the device identifier to the router for subsequent connection without a need for the mobile device or the proxy application.

13. The computer-implemented method of claim 12, further comprising: storing, by the router, the device identifier in a credential management system.

14. The computer-implemented method of claim 13, wherein receiving the message from the proxy application with a network password entered by the user further comprises: sending, by the router, a validation request to the credential management system, which validates the network password if a match for the network password is found.

15. The computer-implemented method of claim 12, further comprising: in response to determining that proxy authentication setting is not enabled, sending, by the router, a denial message to the IoT device.

16. The computer-implemented method of claim 12, further comprising: responsive to the IoT device being disconnected from the wireless network, receiving, by the router, the device ID from the IoT device; looking up the device ID and if found, reestablishing network connection with the IoT device without any input from the user or the mobile device.

17. The computer-implemented method of claim 12, wherein receiving, by the router, the authorization request from the IoT device further comprises: automatically determining, by the IoT device, which one of a plurality of detected wireless networks to request access to by selecting the wireless network having a highest signal strength.

18. The computer-implemented method of claim 13, further comprising: in response to the IoT device failing to receive a reply to the authorization request within a predetermined time threshold, sending, by the IoT device, an authentication request to a router of another wireless network having a next highest signal strength until the IoT device finds the router with proxy authentication enabled.

19. A system, comprising:

a router that provides a wireless network and communicates over the wireless network and an Internet;

an Internet-of-Things (IoT) device requiring first time access to the wireless network, the IoT device associated with a device identifier; and

a proxy application executing on a mobile device of a user, the proxy application to act a proxy for the IoT device during a first network authentication attempt with the router, the proxy application configured to:

receive during a registration process, the device identifier associated with the IoT device, the device identifier entered into the proxy application by the;

transmit the device identifier to the router as part of the registration process;

subsequent to the registration process, receive by the proxy application, the device identifier from the router in response to the router receiving an authorization request comprising the device identifier with no network password from the IoT device for access to the wireless network, and the router forwarding the device identifier to the proxy application after determining that the router has proxy authentication enabled; and

prompt the user of the mobile device to enter the network password, and transmit the entered network password in a message to the router, such that in response to the router validating the network password and granting the IoT device access to the wireless network, the IoT device transmits the device identifier to the router for subsequent network connection without a need for the mobile device or the proxy application.

20. The system of claim 19, further comprising an authentication mapper server in communication with the router, and wherein functionality of the proxy application is separated into a first proxy application and a second proxy application, wherein the authentication mapper server stores a mapping between a first application identifier

associated with the first proxy application, a second application identifier associated with the second proxy application, and the device ID.