be installed in IoT device 441 the factory. In some examples, on initial power-up and initial boot-up, IoT device 441 is cryptographically guaranteed to connect to provisioning service 411 only. Also, IoT device 441 stores identity information about itself as well as optional metadata, which may include geolocation, in some examples. Throughout the specification and the claims, the terms “initial boot” and “initial boot-up” refer to the very first time that the IoT device is booted up after manufacture of the IoT device is complete.

[0044] Further, provisioning service 411 may have some method to verify the identity of IoT device 441. The source used to verify the identity of IoT device 411 may provide provisioning service 411 with additional metadata. Provisioning service device 411 may also contain a rule engine used to route an IoT device's provisioning request to the correct IoT hub. For example, one rule may be for all IoT devices within a certain geographic region to be provisioned to an IoT solution located in a certain region. Provisioning service device 411 may be configured with information about how to connect IoT devices to one or more IoT hubs each corresponding to a separate IoT solution.

[0045] In the illustrated example, upon IoT device 441 first being powered on by a customer, step 421 occurs. At step 421, an identification message may be communicated from IoT device 441 to provisioning service 411.

[0046]In some examples, IoT device 441 is manufactured with the URI of provisioning service 411. In some of these examples, step 421 happens upon IoT device 441 first being powered on. Upon IoT device 441 first being powered on, IoT device 441 may send the identification message to provisioning service 411 via the URI of provisioning service 441.

[0047] The identification information includes information that is usable for verifying that IoT device 441 is a valid device to receive IoT services, and may also include information for determining which IoT solution is appropriate for IoT device 441, such as geographical information.

[0048]As shown, step 422 occurs next. At step 422, the provisioning service determines whether or not IoT device 441 is valid. The validity determination is made in different ways in different examples, which will be discussed in greater detail below. If the provisioning service determines that IoT device 441 is not valid, the process ends.

[0049]If, instead, provisioning service 411 determines that IoT device 441 is valid, step 423 occurs. At step 423, provisioning service 411 selects an IoT hub from a plurality of IoT hubs. In some examples, the selection of the IoT hub is based on routing rules. In some examples, geographical location may be a factor in the selection of the IoT hub. For example, the closest appropriate IoT hub may be selected in some examples. Another factor in the selection of the IoT hub may be dependent on which IoT solution is appropriate based on factors relevant to the IoT device and determined by the IoT device manufacturer. For

examples, the new configuration file and the firmware update are automatically installed in IoT device 441. Throughout the specification and the claims, the term “automatically” refers to performing an action automatically without an intervening manual step.

[0054]As a result of process 420, IoT device 441 is provisioned, is fully able to communicate with IoT services, is up-to-date, and is fully updated with the latest firmware and the latest configuration file, even though IoT device 441 may have been sitting in a warehouse for months or years, all of which is accomplished in an automatic manner without any manual steps, and without human intervention.

[0055]After provisioning is complete, in some examples, communications between IoT device 441 and IoT hub 451 may occur directly and in a normal fashion, and provisioning service 411 are not again involved in communications between IoT device 441 and IoT hub 451, unless, in some examples, IoT device 441 needs to be re-provisioned.

[0056]In some examples, IoT device 441 retains cryptographic memory of provisioning service 411 and can be redirected to provisioning service 411 during the lifetime of IoT device 441 in order to re-provision IoT device 411. In some examples, certain events may cause IoT device 441 to initiate re-provisioning, such as IoT device 441 being resold, a change in geographical regions, or the like.

[0057]In some examples, re-provisioning of an IoT device may be performed as follows. First, a determination is made as to which new IoT hub the IoT device should be attached to (in base data). The term "base data" as used herein refers to data and/or metadata about the IoT device to be used when provisioning the IoT device, such as, for example, location information such as geolocation, device identity information, other suitable metadata, and/or the like. Next, the IoT device is provisioned in the new IoT hub. Then, the new connection information is returned. The IoT device is then deleted from the registry of the old IoT hub.

[0058]In some examples, as a security measure, provisioning service 411 may be restricted from directly connecting to a device without first being contacted by that device. In other examples, provisioning service 411 can directly connect to IoT device 441 without being contacted by IoT device 441, and the security is ensured in some other manner.

[0059JFIG. 5 is a block diagram illustrating an example of a portion (501) of system 300 of FIG. 3. Portion 501 includes IoT device 541, provisioning service 511, and IoT hubs 551 and 552. As shown, provisioning service 511 includes routing rules 591 and enrollment list 592. Also, IoT hub 551 includes device registry 593 and IoT hub 552 includes device registry 594.

[0060]In some examples, IoT device 541 is manufactured with the URI of provisioning service 511 installed therein.

We claim :

1. An apparatus for Internet of Things (IoT) communications, comprising:

a first IoT device, including:

a memory adapted to store run-time data for the first IoT device; and

at least one processor that is adapted to execute processor-executable code that, in response to execution, enables the first IoT device to perform actions, including:

responsive to an initial boot, automatically sending identification information to a provisioning service endpoint stored in the first IoT device, wherein the identification information includes an identification (ID) of the first IoT device;

receiving cryptographic information from the provisioning service endpoint, wherein the cryptographic information is associated with an IoT hub selected from a plurality of IoT hubs based, in part, on the ID of the first IoT device;

automatically sending a message to the IoT hub in response to receiving the cryptographic information;

receiving a new configuration file and a firmware update from the IoT hub without requiring a user association; and

automatically installing the new configuration file and the firmware update.

2. The apparatus of claim 1, wherein the identification information further includes geographical information associated with the first IoT device, and wherein the IoT hub is selected from the plurality of IoT hubs further based upon the geographical information associated with the first IoT device.

3. The apparatus of claim 1, wherein the cryptographic information includes connectivity information associated with the first IoT device connecting to the IoT hub.

4. The apparatus of claim 1, wherein the cryptographic information includes credentials, and wherein the cryptographic information further includes a hostname associated with the IoT hub.

5. The apparatus of claim 1, wherein the actions further include, via communication with the IoT hub, syncing metadata stored in the first IoT device with metadata stored in the IoT hub via device management syncing.

6. The apparatus of claim 1, wherein the identification information includes a certificate that includes the ID of the first IoT device.

7. The apparatus of claim 6, wherein the certificate further includes a Uniform Resource Indicator of the provisioning service endpoint.

8. A method for Internet of Things (IoT) communications, comprising:

responsive to an initial boot, automatically sending identification information to a provisioning service end-point stored in a first IoT device, wherein the identification information includes an identification (ID) of the first IoT device;

receiving cryptographic information from the provisioning service endpoint, wherein the cryptographic information is associated with an IoT hub selected from a plurality of IoT hubs based, in part, on the ID of the first IoT device;

automatically sending a message to the IoT hub in response to receiving the cryptographic information;

receiving a new configuration file and a firmware update from the IoT hub without requiring a user association; and

automatically installing the new configuration file and the firmware update.

9. The method of claim 8, wherein the identification information further includes geographical information associated with the first IoT device, and wherein the IoT hub is selected from the plurality of IoT hubs further based upon the geographical information associated with the first IoT device.

10. The method of claim 8, wherein the cryptographic information includes connectivity information associated with the first IoT device connecting to the IoT hub.

11. The apparatus of claim 8, wherein the cryptographic information includes credentials, and wherein the cryptographic information further includes a hostname associated with the IoT hub.

12. The method of claim 8, further comprising :

via communications with the IoT hub, syncing metadata stored in the first IoT device with metadata stored in the IoT hub via device management syncing

13. The method of claim 8, wherein the identification information includes a certificate that includes the ID of the first IoT device.

14. The method of claim 13, wherein the certificate further includes a Uniform Resource Indicator of the provisioning service endpoint.

15. A processor-readable storage medium having instructions stored therein that, when executed by a first IoT device, cause the first IoT device to perform operations, the operations comprising :

responsive to an initial boot, automatically sending identification information to a provisioning service end-point stored in a first IoT device, wherein the identification information includes an identification (ID) of the first IoT device;

receiving cryptographic information from the provisioning service endpoint, wherein the cryptographic information is associated with an IoT hub selected from a plurality of IoT hubs based, in part, on the ID of the first IoT device;

automatically sending a message to the IoT hub in response to receiving the cryptographic information;

receiving a new configuration file and a firmware update from the IoT hub without requiring a user association; and

automatically installing the new configuration file and the firmware update.

16. The processor-readable storage medium of claim 15, wherein the identification information further includes geographical information associated with the first IoT device , and wherein the IoT hub is selected from the plurality of IoT hubs further based upon the geographical information associated with the first IoT device.

17. The processor-readable storage medium of claim 15, wherein the cryptographic information includes connectivity information associated with the first IoT device connecting to the IoT hub.

18. The processor-readable storage medium of claim 15, wherein the cryptographic information includes credentials, and wherein the cryptographic information further includes a hostname associated with the IoT hub.

19. The processor-readable storage medium of claim 15, wherein the operations further include :

via communication with the IoT hub, syncing metadata stored in the first IoT device with metadata stored in the IoT hub via device management syncing.

20. The processor-readable storage medium of claim 15, wherein the identification information includes a certificate that includes the ID of the first IoT device.