March 2022

MULTI-FACTOR AUTHENTICATION IN A NEXT GENERATION MESH NETWORK

Harbor Dong

Li Zhao

Huimin She

Wenchuan Ji

MULTI-FACTOR AUTHENTICATION IN A NEXT GENERATION MESH NETWORK

AUTHORS:
Harbor Dong
Li Zhao
Huimin She
Wenchuan Ji

ABSTRACT

Security challenges arise when devices (such as, for example, smart meters) that are deployed to Internet of things (IoT) networks employ only a certificate for authentication. A certificate is a static authentication method, and if the security mechanism of a single node is cracked then the security mechanism of the entire IoT network will be broken. At the same time, since the security certificates of all of the nodes are the same it is difficult to isolate and remove the compromised nodes. To address such challenges, techniques are presented herein that support an innovative multi-factor authentication facility. Among other things, the presented techniques leverage the characteristics of a mesh network and are compatible with existing devices (e.g., smart meters).

DETAILED DESCRIPTION

Tens of millions of smart meters have been deployed all over the world during the past ten years. In all of those deployments, nodes have only used certificates for authentication. A certificate is a static authentication method, and in the just-described context if the security mechanism of a single node is cracked then the security mechanism of the entire Internet of things (IoT) network will be broken. At the same time, since the security certificates of all of the nodes are the same it is difficult to isolate and remove the compromised nodes.

Recently, the number of smart meters has increased exponentially. As a result, equipment manufacturers are very concerned about the cost of their IoT equipment. Consequently, manufacturers are looking for a method that does not increase costs but that

can improve safety performance. Among other things, such a method needs to be compatible with existing smart meters.

Based on the above two points, and leveraging the characteristics of a mesh network, techniques are presented herein that support an innovative multi-factor authentication facility.

The presented techniques take advantage of, among other things, the fact that after IoT devices are deployed they typically do not move. Accordingly, following their deployment IoT devices may, according to aspects of the presented techniques, make use of their components (including, for example, a Global Positioning System (GPS) facility or an antenna) to detect their unique physical environment fingerprint (PEF). According to further aspects of the presented techniques, devices may periodically report their PEF to a network management server (NMS) which may maintain the historical data of the PEF of different devices. An NMS may then use that data to generate a pattern of the physical environment of a device. According to still further aspects of the presented techniques, when a device is again authenticated a security mechanism can let the device meter carry real-time dynamic environment fingerprint variables as a part of the authentication factors and an NMS may then employ pattern recognition capabilities, or other methods, to help the security system confirm the identity of the device.

The next section of the instant narrative provides a detailed process description for, along with an exemplary architecture for, aspects of the techniques presented herein.

To begin, when an IoT device wishes to join a mesh network the device must first be authenticated. Such a device may report its certificate to a Remote Authentication Dial-In User Service (RADIUS) server or to a security service system. The security service system may then verify the certificate. If the certificate is illegal, then the access application may be rejected. Otherwise, the process may proceed to the next step.

Next, an NMS may be checked for the existence of PEF pattern (which will be described below). If such a pattern exists, then the security service system may ask the node to report its real-time PEF to the NMS. Since the real-time PEF is a dynamic value, the instant process (according to aspects of the techniques presented herein) is, as a result, also dynamic. If the pattern does not exist, then the first few applications may be exempted. Otherwise, the access application may be rejected.

Subsequently, when the NMS receives the PEF report, the NMS may employ a pattern recognition method, or other methods, to confirm the validity of the PEF. If the PEF does not match the record of the pattern, then the NMS may send the result to the security service system where the security service may reject the application and delete the credit of the node certificate. Otherwise, the process may proceed to the next step.

Next, the security system may use the pattern to create a set of challenges, regarding the node's physical environment, which the security system may use to challenge the IoT device. For example, an inquiry may be made as to whether smart meter A is able to hear the signal of smart meter B. If smart meter A can indeed hear smart meter B, then the security system may ask smart meter A to ask smart meter B to report data to the NSM or the security system. Importantly, such a process it is not considered successful until the challenge is passed. Further, since a challenge set is randomly generated the instant process (according to aspects of the techniques presented herein) is, as a result, also dynamic.

Finally, after joining a network devices may periodically report their PEF to the NMS so that the NMS may generate a PEF pattern.

Figure 1, below, depicts elements of an exemplary process flowchart according to aspects of the techniques presented herein and reflective of the above discussion.

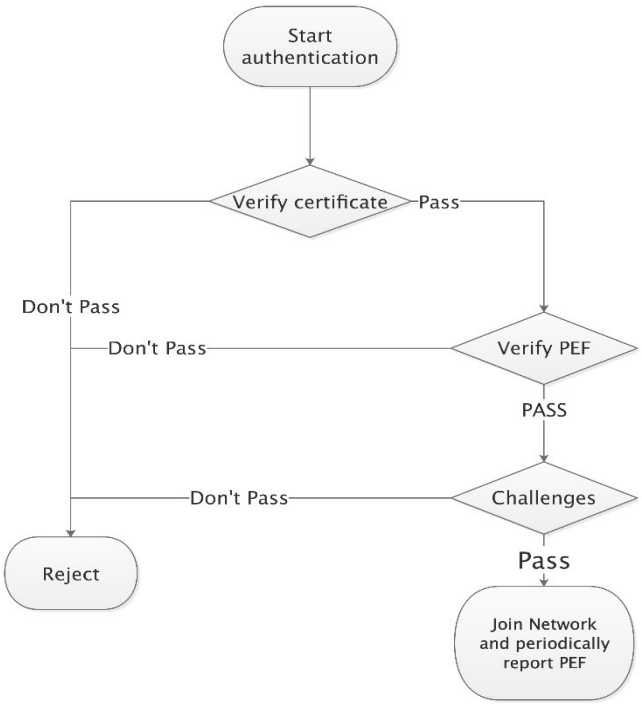

Figure 1: Exemplary Process Flowchart

As described above, aspects of the techniques presented herein encompass a PEF. Such an artifact may include all of the environmental factors that may be detected by a node's components. Examples of such factors may include, possibly among other things, a radio frequency link quality, an Received Signal Strength Indicator (RSSI) level, and background noise which are detected by an antenna; light energy that may be detected by a photovoltaic cell; an absolute address (as detected through a GPS facility) and a relative address (that may be calculated through a signal strength algorithm); and the number and behaviors of neighbors which are detected by radio frequency (RF) components.

As noted previously, aspects of the techniques presented herein employ a pattern that may be generated from a PEF. In support of such a pattern, IoT devices may periodically report their PEF to an NMS thus providing the NMS with historical PEF data. From that data the NMS may extract a feature value or matrix to generate a pattern of the individual PEF of an IoT device.

At the same time, every IoT device has an overlapping space with other devices. Figure 2, below, illustrates elements of such an overlap area.

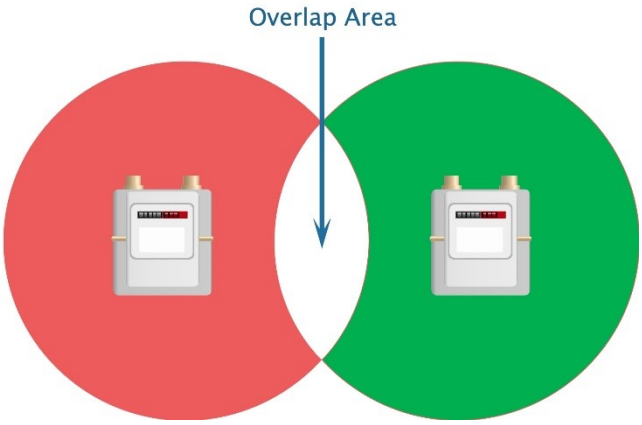

Figure 2: Illustrative Overlap

Consequently, it is possible, according to aspects of the techniques presented herein, to develop a correlation matrix of PEFs between each IoT device. An NMS may extract the overlap of PEFs to generate a pattern of the overlap PEF between each IoT device.

As noted previously, aspects of the techniques presented herein employ a mechanism for determining whether a PEF matches a pattern.

First, a device's PEF may be matched to the pattern of the individual PEF. If a device has been compromised, then a hacker will have copied this device and deployed it in other areas. Importantly, the new area's PEF will not match to the existing pattern. An NMS may check the database of devices where it will find that this device's security information has been cracked. As a result, this suite of security certificates must be unregistered.

Next, a device's PEF may be matched to the pattern of the overlap PEF. If a device has been compromised, then a hacker will have copied this device and deployed it in the same areas. The individual part of a PEF may be matched during the above-described first step. However, because the number of devices in this area has increased, the overlapping PEF will not match to the overlap PEF's pattern. An NMS may traverse more patterns of the overlap space to locate the suspicious device (even if the hacker has not added new devices but is just controlling the cracked devices). Since hackers will force devices to perform some irregular behaviors, those irregular behaviors will change the uncracked devices' overlap PEF. When an uncracked device reports its PEF, the NMS will find that its PEF does not match and the NMS may perform a further investigation to find the cracked device.

As described and illustrated in the above narrative, the techniques presented herein encompass a number of capabilities that are of interest and note. For example, in addition to the physical properties of a device itself, a PEF (according to the presented techniques) includes all of the environmental factors that can be detected by a node's components. Existing solutions only focus on using device fingerprinting. In contrast, the presented techniques include the characteristics of the physical environment in which a device is located. Such characteristics may include a radio frequency link quality, an RSSI level, and background noise which are detected by an antenna; light energy that may be detected by a photovoltaic cell; an absolute address (as detected through a GPS facility) and a relative address (that may be calculated through a signal strength algorithm); and the number and behaviors of neighbors which are detected by RF components.

Further, aspects of the presented techniques extract an individual pattern from each PEF and also develop a correlation pattern between each PEF. Such a correlation pattern has the effect of providing a reciprocal verification between devices. Additionally, in

contrast to existing multi-factor authentication solutions (which only use cryptography or matching) aspects of the presented techniques dynamically generate a question set. A device may be asked to answer various of such questions. Additionally, such questions may even include behavior verification.

In summary, techniques have been presented that support an innovative multi-factor authentication facility. Among other things, the presented techniques leverage the characteristics of a mesh network and are compatible with existing devices (e.g., smart meters). Aspects of the presented techniques employ a device's unique PEF which, in contrast to existing solutions, encompasses not just a device's physical properties but also various environmental factors that may be detected by a node's components. Such factors, reflecting the physical environment in which the device is located, may include a radio frequency link quality, an RSSI level, and background noise which are detected by an antenna; light energy that may be detected by a photovoltaic cell; an absolute address (as detected through a GPS facility) and a relative address (that may be calculated through a signal strength algorithm); and the number and behaviors of neighbors which are detected by radio frequency RF components. Further aspects of the presented techniques extract an individual pattern from each PEF and also develop a correlation pattern between each PEF (where such a correlation pattern has the effect of providing a reciprocal verification between devices). Still further aspects of the presented techniques dynamically generate a question set (that may, for example, include behavior verification) that may be used to challenge a device.