CLAIMS

What is claimed is:

1. A security detection device, wherein the security detection device is configured to detect an Internet of Things (IoT) device in an IoT network, and the security detection device comprises:

a software wireless unit, configured to monitor a wireless signal sent by the IoT device to obtain a wireless message, wherein the wireless message comprises a first verification code generated by the IoT device; and

an analysis unit, configured to:

determine a target running feature of the IoT device by using the wireless message, wherein determining the target running feature of the IoT device comprises:

generating a second verification code,

performing a security check of the wireless message based on the first verification code and the second verification code,

determining that the security check fails,

responsive to determining that the security check fails, performing an additional security check of the wireless message based on a private verification rule,

determining that the additional security check succeeds, and

subsequent to determining that the additional security check succeeds,

parsing the first verification code to obtain a parsing result, and

obtaining a private message from the wireless message based on the parsing result, and

compare the target running feature with a historical normal running feature of the IoT device to determine whether the IoT device runs abnormally.

2. The device according to claim 1, wherein the target running feature/ or the historical normal running feature comprises one or more of the following:

a quantity variation feature of IoT devices in an IoT network, an IoT device's wireless message recipient feature, an IoT device's wireless message throughput variation feature, an IoT device's sign-in and sign-off time feature, or an IoT device's service feature.

~~3. The device according to claim 1, wherein the determine the target running feature of the IoT device by using the wireless message comprises:~~

~~if a verification code fails to be verified by verification rules provided by a predetermined communications protocol, but is subsequently verified by private rules, determining that the target running feature of the IoT device includes transmitting a private message.~~

3~~4~~. The device according to claim 1, wherein the target running feature or ~~/~~the historical normal running feature comprises one or more of the following attack features:

an attack instruction feature, a specified attack behavior feature, or an interference signal feature.

4~~5~~. The device according to claim 1, wherein a hardware capability~~/~~ or a computing capability of the IoT device is less than a specified parameter.

5~~6~~. A security detection method, wherein the method comprises:

obtaining a wireless message of an Internet of Things (IoT) device, wherein the wireless message is obtained by monitoring, by using a software wireless technology, a wireless signal sent by the IoT device, and wherein the wireless message comprises a first verification code generated by the IoT device; and

determining a target running feature of the IoT device by using the wireless message, wherein determining the target running feature of the IoT device comprises:

generating a second verification code,

performing a security check of the wireless message based on the first verification code and the second verification code,

determining that the security check fails,

responsive to determining that the security check fails, performing an additional security check of the wireless message based on a private verification rule,

determining that the additional security check succeeds, and

subsequent to determining that the additional security check succeeds,

parsing the first verification code to obtain a parsing result, and

obtaining a private message from the wireless message based on the parsing result, and

comparing the target running feature with a historical normal running feature of the IoT device to determine whether the IoT device runs abnormally.

67. The method according to claim 56, wherein the target running feature or /the historical normal running feature comprises one or more of the following:

a quantity variation feature of IoT devices in an IoT network, an IoT device's wireless message recipient feature, an IoT device's wireless message throughput variation feature, an IoT device's sign-in and sign-off time feature, or an IoT device's service feature.

~~8. The method according to claim 6, wherein the determining a target running feature of the IoT device by using the wireless message comprises:~~

~~if a verification code fails to be verified by verification rules provided by a predetermined communications protocol, but is subsequently verified by private rules, determining that the target running feature of the IoT device includes transmitting a private message.~~

79. The method according to claim 56, wherein the target running feature or /the historical normal running feature comprises one or more of the following attack features:

an attack instruction feature, a specified attack behavior feature, or an interference signal feature.

810. The method according to claim 56, wherein a hardware capability or/ a computing capability of the IoT device is less than a specified level.

911. A security detection apparatus, wherein the apparatus comprises:

an acquisition module, configured to obtain a wireless message of an Internet of Things (IoT) device, wherein the wireless message is obtained by monitoring, by using a software wireless technology, a wireless signal sent by the IoT device, and wherein the wireless message comprises a first verification code generated by the IoT device; and

a determining module, configured to determine a target running feature of the IoT device by using the wireless message, wherein determining the target running feature of the IoT device comprises:

generating a second verification code,

performing a security check of the wireless message based on the first verification code and the second verification code,

determining that the security check fails,

responsive to determining that the security check fails, performing an additional security check of the wireless message based on a private verification rule,

determining that the additional security check succeeds, and

subsequent to determining that the additional security check succeeds,

parsing the first verification code to obtain a parsing result, and

obtaining a private message from the wireless message based on the parsing result, and

compare the target running feature with a historical normal running feature of the IoT device to determine whether the IoT device runs abnormally.

10~~12~~. A security detection device, comprising a software wireless processor, a memory, a main processor, and a computer program that is stored in the memory and that is capable of running on the main processor, wherein when executing the program, the main processor implements the following method:

obtaining a wireless message of an Internet of Things (IoT) device, wherein the wireless message is obtained by monitoring, by using the software wireless processor, a wireless signal sent by the IoT device, and wherein the wireless message comprises a first verification code generated by the IoT device; and

determining a target running feature of the IoT device by using the wireless message, wherein determining the target running feature of the IoT device comprises:

generating a second verification code,

performing a security check of the wireless message based on the first verification code and the second verification code,

determining that the security check fails,

responsive to determining that the security check fails, performing an additional security check of the wireless message based on a private verification rule,

determining that the additional security check succeeds, and

subsequent to determining that the additional security check succeeds,

parsing the first verification code to obtain a parsing result, and

obtaining a private message from the wireless message based on the parsing result, and

comparing the target running feature with a historical normal running feature of the IoT device to determine whether the IoT device runs abnormally.