# DATA REPORTING METHOD AND SYSTEM FOR MODBUS PROTOCOL DEVICE

## TECHNICAL FIELD

**[0001]** The present invention relates to the technical field of data transmission, and particularly relates to a data reporting method and system for a Modbus protocol device.

## BACKGROUND

**[0002]** In an Internet of Things (IoT) cloud platform, a terminal device needs to report its attribute information proactively. The attribute information refers to parameters used to describe statuses or characteristics of the terminal device, such as temperature, humidity, or electric quantity.

**[0003]** Currently, a Modbus protocol terminal device in an IoT architecture using a Modbus protocol needs to read its device attribute proactively, and encapsulate data of the terminal device before loading the same to the IoT cloud platform for status analysis, so as to determine whether the terminal device is online and whether it is in an abnormal status.

**[0004]** As shown in FIG. 3 of the accompanying drawings of the specification, no interface suitable for the terminal device in the Modbus protocol to proactively upload its attribute information is available. Moreover, a devices in a Modbus protocol gateway does not proactively send its status and attribute information to the IoT cloud platform either, and the IoT cloud platform cannot proactively obtain the status and attribute information from the device. In addition, the Modbus protocol itself has neither a data encryption mechanism nor a verification mechanism, resulting in security risks when the device transmits data via the Modbus protocol.

## SUMMARY OF THE INVENTION

**[0005]** The present invention provides a data reporting method and system for a Modbus protocol device, which can ensure the automatic data reporting of the Modbus protocol devices and the security of data reporting.

**[0006]** In order to achieve the above objectives, the present invention provides a Modbus protocol Internet of Things (IoT) system, including:

an IoT cloud platform, a Modbus gateway adaptation layer, a Modbus gateway, and a plurality of terminal devices, where the IoT cloud platform is connected to the Modbus gateway adaptation layer, the Modbus gateway adaptation layer is connected to the Modbus gateway, and the Modbus gateway is connected to the plurality of terminal devices.

**[0007]** Optionally, the Modbus gateway adaptation layer is integrated in the Modbus gateway.

**[0008]** Optionally, the IoT cloud platform and the Modbus gateway adaptation layer communicate in a bidirectional way, and the Modbus gateway adaptation layer and the Modbus gateway also communicate in a bidirectional way.

**[0009]** In order to solve the above problems, the present invention further provides a data reporting method for a Modbus protocol device based on the Modbus protocol IoT system, including:

sending a connection packet to the IoT cloud platform when the gateway adaptation layer is activated, where the connection packet includes a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer;

obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer, screening out device status data from the connection

data according to the heartbeat packet interval, and encrypting the device status data to obtain encrypted device status data;

screening out device attribute function data from the connection data according to the device code, and encrypting the device attribute function data to obtain encrypted device attribute data; and

uploading the encrypted device status data and the encrypted device attribute data to the IoT cloud platform to complete data reporting.

**[0010]** Optionally, after the sending a connection packet to the IoT cloud platform when the gateway adaptation layer is activated further includes:

the IoT cloud platform receives and parses the connection packet to obtain a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer; and

the IoT cloud platform modifies a status of the terminal device that matches the device code in the gateway adaptation layer to an online status, and stores the heartbeat packet interval indicated in the connection packet.

**[0011]** Optionally, before the obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer further includes:

determining a function point and a device code of the gateway adaptation layer according to preset business requirements;

configuring gateway architecture of the gateway adaptation layer according to the function point and the device code;

writing a function code for the gateway architecture using a preset coding method; and

integrating the function point, the device code, the gateway architecture, and the function code to obtain a data point.

**[0012]** Optionally, the screening out device status data from the connection data according to the heartbeat packet interval includes:

polling all the terminal devices in the gateway adaptation layer during a first heartbeat packet interval time period;

extracting device status data of the terminal devices whose return data is in a normal status; and

storing the device status data in the heartbeat packet, and encrypting the heartbeat packet using a preset encryption algorithm to obtain encrypted device status data.

**[0013]** Optionally, the screening out device attribute function data from the connection data according to the device code includes:

polling the device attribute function data proactively in the gateway adaptation layer during a second heartbeat packet interval time period; and

encrypting the device attribute function data using the preset encryption algorithm to obtain encrypted device attribute data.

**[0014]** Optionally, after obtaining encrypted device status data also includes:

uploading the encrypted device status data to the IoT cloud platform, and parsing the encrypted device status data by using the IoT cloud platform to identify an online status of the device;

caching the device data that does not contain the device code in the heartbeat packet by using the IoT cloud platform, recording a number of times the heartbeat packet has not been received, and determining whether the device is in the online status according to the number of times;

when the number of times exceeds a preset warning threshold for the number of times, a device that does not contain the device code in heartbeat packet is determined to be in an offline status;

when the number of times does not exceed the preset warning threshold for the number of times, the IoT cloud platform sends an inquiry request to the gateway adaptation

layer during a first preset warning time period, and waits for the gateway adaptation layer to respond to the device status data of the device; and

when the gateway adaptation layer does not give a response, it indicates that all the terminal devices in the gateway adaptation layer are in the offline status.

**[0015]** Optionally, the obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer includes:

extracting a data packet of the gateway adaptation layer according to the data point configured in the gateway adaptation layer;

extracting the device code from the data packet, and extracting the connection packet corresponding to the device code when the gateway adaptation layer is activated; and

polling the device corresponding to the device code according to the heartbeat packet interval of the connection packet, and extracting the device code and corresponding attribute data of the device in a normal status when the device status is normal to obtain the connection data.

**[0016]** By deploying the gateway adaptation layer in a local area network, this embodiment can process the data from the device and the IoT cloud platform via the gateway adaptation layer as a processing medium for data reporting, obtain the connection data of the terminal device corresponding to the device code by using the gateway adaptation layer, and automatically obtain the device data and then report the data via the gateway adaptation layer. In addition, the device status data and the device attribute function data can be encrypted to ensure the security of data reporting.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0017]** FIG. 1 is a schematic flow diagram of a data reporting method for a Modbus protocol device according to an embodiment of the present invention.

**[0018]** FIG. 2 is a schematic diagram of a Modbus protocol IoT system according to an embodiment of the present invention.

**[0019]** FIG. 3 is a schematic diagram of a system currently applicable to terminal devices in a Modbus protocol according to an embodiment of the present invention.

**[0020]** Implementation, functional features and advantages of the objective of the present invention will be further described with reference to the accompanying drawings in connection with the embodiments.

## DETAILED DESCRIPTION

**[0021]** It should be understood that particular embodiments described herein are merely illustrative of the present invention, and are not intended to limit the present invention.

**[0022]** With reference to FIG. 1, a schematic flow diagram of a data reporting method for a Modbus protocol device illustrated in an embodiment of the present invention is provided. In this embodiment, the data reporting method for a Modbus protocol device includes:

S1. send a connection packet to an Internet of Things (IoT) cloud platform when a gateway adaptation layer is activated, where the connection packet includes a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer.

**[0023]** In this embodiment, the IoT refers to a computer communication network that enables data sharing and transmission among terminal devices in a same geographical area.

**[0024]** In this embodiment, the gateway adaptation layer refers to a gateway layer in software architecture. For example, in this embodiment, a Modbus gateway adaptation layer is adopted, the Modbus gateway adaptation layer refers to an adapter that uses a Modbus protocol for communication, and the Modbus gateway adaptation layer can be used to communicate between buses or networks that use the Modbus protocol.

**[0025]** In this embodiment, the heartbeat packet interval refers to interval time at which the terminal device sends a heartbeat packet to a server platform in network communication. For example, a complete heartbeat packet interval refers to a period of time from a device end sending the server platform a heartbeat packet to a time point when a next heartbeat packet is sent.

**[0026]** As an embodiment of the present invention, the send a connection packet to an Internet of Things (IoT) cloud platform when a gateway adaptation layer is activated includes:

the IoT cloud platform receives and parses the connection packet to obtain a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer; and

the IoT cloud platform modifies a status of the terminal device that matches the device code in the gateway adaptation layer to an online status, and stores the heartbeat packet interval indicated in the connection packet.

**[0027]** In this embodiment, the IoT cloud platform refers to a network platform that combines an IoT cloud platform and cloud computing technology, which is capable of performing downward connection and management of the terminal device in the IoT, and uploading and storing data of the terminal device.

**[0028]** S2. obtain connection data of the terminal device corresponding to the device code by using the gateway adaptation layer, screen out device status data from the connection data according to the heartbeat packet interval, and encrypt the device status data to obtain encrypted device status data.

**[0029]** In this embodiment, the device status data refers to an operating status of the terminal device in the gateway adaptation layer, including online status and offline status.

**[0030]** As an embodiment of the present invention, before obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer further includes:

determine a function point and a device code of the gateway adaptation layer according to preset business requirements;

configure gateway architecture of the gateway adaptation layer according to the function point and the device code;

write a function code for the gateway architecture using a preset coding method; and

integrate the function point, the device code, the gateway architecture, and the function code to obtain a data point.

**[0031]** In this embodiment, the function point refers to a data interaction unit in the Modbus protocol. In Modbus communication, a device can contain a plurality of function points, each of the function point corresponds to one specific data item or operation. The function point is used to identify a location of data to be read or written, or the operation to be performed.

**[0032]** In this embodiment, the device code refers to a device identifier in a Modbus network. Each device in the Modbus network has a unique device code to distinguishing it from other devices. The device code ranges from 1 to 247, where 1 to 127 are standard device codes, and 128 to 247 are user-defined device codes.

**[0033]** In this embodiment, the function code refers to an operation code defined in the Modbus protocol, which is used to specify a type of operation to be performed. The function code indicates specific operation to be performed on the function point, such as reading data, writing data, or setting parameters. Different function codes correspond to different functions, for example, function code 3 indicates reading values of a plurality of holding registers, and function code 6 indicates writing a value of a single holding register.

**[0034]** Further, the obtain connection data of the terminal device corresponding to the device code by using the gateway adaptation layer includes:

extract a data packet of the gateway adaptation layer according to the data point configured in the gateway adaptation layer;

extract the device code from the data packet, and extract the connection packet corresponding to the device code when the gateway adaptation layer is activated; and

poll the device corresponding to the device code according to the heartbeat packet interval of the connection packet, and extract the device code and corresponding attribute data of the device in a normal status when the device status is normal to obtain the connection data.

**[0035]** As an embodiment of the present invention, the screen out device status data from the connection data according to the heartbeat packet interval includes:

poll all the terminal devices in the gateway adaptation layer during a first heartbeat packet interval time period;

extract device status data of the terminal devices whose return data is in a normal status; and

store the device status data in the heartbeat packet, and encrypt the heartbeat packet using a preset encryption algorithm to obtain encrypted device status data.

**[0036]** In this embodiment, the first heartbeat packet interval time period refers to polling time set for polling the device, where the first heartbeat packet interval time period can be calculated using the following formula:

first heartbeat packet interval time period ＝2* number of devices + random number + fault tolerance time.

**[0037]** Specifically, the number of devices refers to a number of devices in the gateway adaptation layer, the random number is a randomly selected positive value, and the fault tolerance time is a time range set to ensure polling accuracy.

**[0038]** In this embodiment, the preset encryption algorithm refers to a method by which the gateway adaptation layer encrypts the data before the data is uploaded to the IoT cloud platform, for example, the preset encryption algorithm can adopt an AES encryption algorithm.

**[0039]** Further, after obtaining encrypted device status data also includes:

upload the encrypted device status data to the IoT cloud platform, and parse the encrypted device status data by using the IoT cloud platform to identify an online status of the device;

cache the device data that does not contain the device code in the heartbeat packet by using the IoT cloud platform, record a number of times the heartbeat packet has not been received, and determine whether the device is in the online status according to the number of times;

when the number of times exceeds a preset warning threshold for the number of times, a device that does not contain the device code in heartbeat packet is determined to be in an offline status;

when the number of times does not exceed the preset warning threshold for the number of times, the IoT cloud platform sends an inquiry request to the gateway adaptation layer during a first preset warning time period, and waits for the gateway adaptation layer to respond to the device status data of the device; and

when the gateway adaptation layer does not give a response, it indicates that all the terminal devices in the gateway adaptation layer are in the offline status.

**[0040]** In this embodiment, the preset warning threshold for the number of times can be set to 2.

**[0041]** S3. screen out device attribute function data from the connection data according to the device code, and encrypt the device attribute function data to obtain encrypted device attribute data.

**[0042]** In this embodiment, the device attribute function data refers to parameters used to describe statuses or characteristics of the terminal device, such as temperature, humidity, or electric quantity.

**[0043]** As an embodiment of the present invention, the screen out device attribute function data from the connection data according to the device code includes:

poll all the device attribute function data proactively in the gateway adaptation layer during a second heartbeat packet interval time period; and

encrypt the device attribute function data using the preset encryption algorithm to obtain encrypted device attribute data.

**[0044]** In this embodiment, the second heartbeat packet interval time period refers to polling time set for polling the device attribute, where the second heartbeat packet interval time period can be calculated using the following formula:

second heartbeat packet interval time period ＝2* number of devices + random number.

**[0045]** S4. upload the encrypted device status data and the encrypted device attribute data to the IoT cloud platform to complete data reporting.

**[0046]** By deploying the gateway adaptation layer in a local area network, this embodiment can process the data from the device and the IoT cloud platform via the gateway adaptation layer as a processing medium for data reporting, obtain the connection data of the terminal device corresponding to the device code by using the gateway adaptation layer, and

automatically obtain the device data and then report the data via the gateway adaptation layer. In addition, the device status data and the device attribute function data can be encrypted to ensure the security of data reporting.

**[0047]** With reference to FIG. 2, a schematic diagram of a Modbus protocol IoT system illustrated in an embodiment of the present invention is provided. In this embodiment, the Modbus protocol IoT system includes:

an IoT cloud platform, a Modbus gateway adaptation layer, a Modbus gateway, and a plurality of terminal devices, where the IoT cloud platform is connected to the Modbus gateway adaptation layer, the Modbus gateway adaptation layer is connected to the Modbus gateway, and the Modbus gateway is connected to the plurality of terminal devices; the Modbus gateway adaptation layer is integrated in the Modbus gateway; and the IoT cloud platform and the Modbus gateway adaptation layer communicate in a bidirectional way, and the Modbus gateway adaptation layer and the Modbus gateway also communicate in a bidirectional way.

**[0048]** For those skilled in the art, it is apparent that the present invention is not limited to details of the exemplary embodiments, and the present invention can be implemented in other specific forms without departing from the spirit or basic features of the present invention.

**[0049]** Therefore, the embodiments should be regarded as illustrative and non-restrictive no matter from which point of view. The scope of the present invention is defined by the appended claims rather than the above specification, and therefore, it is intended that all changes which fall within the meaning and scope of equivalency of the claims are embraced in the present invention. Any reference numerals related to the accompanying drawings in the claims should not be construed as limiting the claims to which they relate.

**[0050]** In addition, it is obvious that the term "including" does not exclude other units or steps, and the singular form does not exclude the plural. Multiple units or devices stated in the system claims can also be implemented by a single unit or device through software or hardware. Terms such as "first" and "second" are used to indicate names and do not imply any specific order.

**[0051]** Finally, it should be noted that the above embodiments are merely intended for describing the technical solutions of the present invention rather than limiting same. Although the present invention is described in detail with reference to the above embodiments, persons of ordinary skill in the art should understand that they may still make modifications or equivalent replacements to the technical solutions of the present invention without departing from the spirit and scope of the technical solutions of the present invention.

**CLAIMS**

1. A Modbus protocol IoT system, characterized by comprising

an IoT cloud platform, a Modbus gateway adaptation layer, a Modbus gateway, and a plurality of terminal devices, the IoT cloud platform is connected to the Modbus gateway adaptation layer, the Modbus gateway adaptation layer is connected to the Modbus gateway, and the Modbus gateway is connected to the plurality of terminal devices.

2. The Modbus protocol IoT system according to claim 1, characterized in that the Modbus gateway adaptation layer is integrated in the Modbus gateway.

3. The Modbus protocol IoT system according to claim 1 or 2, characterized in that the IoT cloud platform and the Modbus gateway adaptation layer communicate in a bidirectional way, and the Modbus gateway adaptation layer and the Modbus gateway also communicate in a bidirectional way.

4. A data reporting method for a Modbus protocol device based on the Modbus protocol IoT system according to any one of claims 1-3, characterized by comprising

sending a connection packet to an IoT cloud platform when a gateway adaptation layer is activated, and the connection packet comprises a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer;

obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer, screening out device status data from the connection data according to the heartbeat packet interval, and encrypting the device status data to obtain encrypted device status data;

screening out device attribute function data from the connection data according to the device code, and encrypting the device attribute function data to obtain encrypted device attribute data; and

uploading the encrypted device status data and the encrypted device attribute data to the IoT cloud platform to complete data reporting.

5. The data reporting method for a Modbus protocol device according to claim 4, characterized in that after the sending a connection packet to the IoT cloud platform when the gateway adaptation layer is activated further comprises:

the IoT cloud platform receives and parses the connection packet to obtain a device code and a heartbeat packet interval of one terminal device configured in the gateway adaptation layer; and

the IoT cloud platform modifies a status of the terminal device that matches the device code in the gateway adaptation layer to an online status, and stores the heartbeat packet interval indicated in the connection packet.

6. The data reporting method for a Modbus protocol device according to claim 4, characterized in that before the obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer further comprises:

determining a function point and a device code of the gateway adaptation layer according to preset business requirements;

configuring gateway architecture of the gateway adaptation layer according to the function point and the device code;

writing a function code for the gateway architecture using a preset coding method; and

integrating the function point, the device code, the gateway architecture, and the function code to obtain a data point.

7. The data reporting method for a Modbus protocol device according to claim 4, characterized in that the screening out device status data from the connection data according to the heartbeat packet interval comprises:

polling all the terminal devices in the gateway adaptation layer during a first heartbeat packet interval time period;

extracting device status data of the terminal devices whose return data is in a normal status; and

storing the device status data in the heartbeat packet, and encrypting the heartbeat packet using a preset encryption algorithm to obtain encrypted device status data.

8. The data reporting method for a Modbus protocol device according to claim 4, characterized in that the screening out device attribute function data from the connection data according to the device code comprises:

polling the device attribute function data proactively in the gateway adaptation layer during a second heartbeat packet interval time period; and

encrypting the device attribute function data using the preset encryption algorithm to obtain encrypted device attribute data.

9. The data reporting method for a Modbus protocol device according to claim 7, characterized in that after obtaining encrypted device status data further comprises:

uploading the encrypted device status data to the IoT cloud platform, and parsing the encrypted device status data by using the IoT cloud platform to identify an online status of the device;

caching the device data that does not contain the device code in the heartbeat packet by using the IoT cloud platform, recording a number of times the heartbeat packet has not been received, and determining whether the device is in the online status according to the number of times;

when the number of times exceeds a preset warning threshold for the number of times, a device that does not contain the device code in heartbeat packet is determined to be in an offline status;

when the number of times does not exceed the preset warning threshold for the number of times, the IoT cloud platform sends an inquiry request to the gateway adaptation layer

during a first preset warning time period, and waits for the gateway adaptation layer to respond to the device status data of the device; and

when the gateway adaptation layer does not give a response, it indicates that all the terminal devices in the gateway adaptation layer are in the offline status.

10. The data reporting method for a Modbus protocol device according to claim 4, characterized in that the obtaining connection data of the terminal device corresponding to the device code by using the gateway adaptation layer further comprises:

extracting a data packet of the gateway adaptation layer according to the data point configured in the gateway adaptation layer;

extracting the device code from the data packet, and extracting the connection packet corresponding to the device code when the gateway adaptation layer is activated; and

polling the device corresponding to the device code according to the heartbeat packet interval of the connection packet, and extracting the device code and corresponding attribute data of the device in a normal status when the device status is normal to obtain the connection data.