NB-IoT物联网表通信标准协议

修订记录

|  |  |  |
| --- | --- | --- |
| **版本** | **日期** | **修改内容** |
| V1.0 | 2018年10月10日 | 第一版 |

1. 范围

本标准对智能远传燃气表的通信协议进行规范。

1. 术语和定义
   1. 主站 master station

指部署在远端的采集服务器。

* 1. 终端设备 terminal device

指具备和远端采集服务器通信的智能燃气表。

* 1. SHA256算法 secure hash algorithm 256

安全哈希算法的一个版本。计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护。

* 1. AES128算法 advanced encryption standard 128 algorithm

一种标准的分组加密对称密钥加密算法。

* 1. HMAC keyed-hash message authentication code

一种带密钥的哈希消息认证码。

1. 网络环境

本协议可部署于基于NB-IoT的网络环境下。本标准对应用层协议进行了规范，对网络传输协议不做强制要求。本标准可基于TCP或者UDP，或者作为CoAP、Http的负载数据。

1. 协议格式
   1. 帧结构

表1 帧结构

|  |  |  |
| --- | --- | --- |
| **字 段** | **长 度** | **代 号** |
| 帧头 | 1 | HEAD |
| 协议类型 | 1 | T |
| 协议框架版本 | 1 | V |
| 帧长度 | 2 | L |
| 消息序号 | 1 | MID |
| 控制域 | 1 | C |
| 数据对象ID | 2 | DID |
| 数据域 | L-12 | D |
| 校验域 | 2 | CRC |
| 帧尾 | 1 | TAIL |

协议中如果没有特殊声明，采用大端格式。

* 1. 帧头（HEAD）

数值为68H，一帧的开始。

* 1. 协议类型（T）

协议类型号。为后期扩展预留。本协议对应的类型号为0。

* 1. 协议框架版本（V）

协议框架的版本号。为后期扩展预留。本协议对应的版本号为1。

* 1. 帧长度（L）

整帧长度，包括帧头。

* 1. 消息序号（MID）

下行报文和最近一次的上行报文一致。燃气表每次发送后数值自增1。

* 1. 数据对象ID （DID）

参考附　录　A

* 1. 控制域 (C)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bit7 | Bit6 | Bit5 | Bit4 | Bit3 | Bit2 | Bit1 | Bit0 |
| 方向 | 后续帧标识 | 保留 | 功能码 | | | | |

Bit7: 方向标识。0——上行报文，1——下行报文

Bit6: 是否有后续帧。0——无后续报文，1——有后续报文

Bit0~Bit4: 功能码。具体内容参考下表。

表2 功能码

|  |  |  |  |
| --- | --- | --- | --- |
| **功能码** | **名称** | **数据域说明** | |
| 01H | 数据上报 | 数据对象（明文或密文）+MAC(部分数据对象有） | |
| 02H | 数据下发 | 数据对象（明文或密文）+MAC(部分数据对象有） | |
| 03H | 续传 | 无数据域 | |
| 04H | 读数据 | 下行 | 无 |
| 上行 | 数据对象（明文或密文）+MAC(部分数据对象有） |
| 05H | 写数据 | 下行 | 数据对象（密文）+MAC |
| 上行 | 2字节错误码（参考附录A.8) |
| 07H | 读记录 | 下行 | 记录数据对象的下行数据（明文或密文）+MAC(部分数据对象有） |
| 上行 | 记录数据对象的上行数据（明文或密文）+MAC(部分数据对象有） |
| 08H | 写回读 | 下行 | 数据对象（密文）+MAC |
| 上行 | 2字节错误码（参考附录A.8)  +回读数据（密文，成功时有） |

数据对象的定义参考附录A。

* 1. 数据域 （D）

1. 加密数据补齐算法

补齐算法使用PKCS7Padding算法

PKCS7Padding：填充的原则是，如果需要N字节补齐，报文长度少于N个字节，需要补满N个字节，补(N-len)个(N-len)。如果报文长度正好时N字节的整数倍，则需要补N个十进制N。

举例：

需要8字节补齐，123这个节符串余3个字节，8-3= 5,补满后如：123+5个十进制的5，如果字符串长度正好是8字节的整数倍，则需要再补8个字节的十进制的8。

本协议采用AES128 ECB加密算法。补齐对齐位数为128位，即16字节。

1. MAC算法

本协议采用“会话MAC密钥”经HMAC-SHA256算法生成MAC。

1. 仅明文

明文传输时，数据域中仅包含数据对象内容。不同数据对象ID对应的数据对象内容参考附录A中的定义。



图1 明文传输

1. 明文+MAC

明文传输且带有MAC信息时，首先在数据对象前面添加上“随机数”（该随机数为数据对象“设备通信参数”中的通信随机码），然后进过MAC算法计算出MAC值。最后将MAC追加在数据对象内容后作为数据域。



图2 明文+MAC

1. 仅密文

当仅密文传输时，首先根据分组加密的分组长度进行数据补齐（补齐算法采用PKCS7标准）。补齐后的数据经过加密生成加密数据域，作为数据域。本协议加密算法选用AES128。



图3 仅密文

1. 密文+MAC

当仅密文传输时，首先根据分组加密的分组长度进行数据补齐（补齐算法采用PKCS7标准）。补齐后的数据经过加密生成加密数据域。随机数+加密数据域经过MAC算法计算出MAC。最后将MAC追加到加密数据域后，生成数据域。



图4 密文+MAC

* 1. 校验域 （CRC）

使用CRC16进行计算。计算算法参考附　录　B。校验范围从“消息序号”到“数据域”

* 1. 帧尾（TAIL）

数值为16H，一帧的结尾。

1. 密钥使用
   1. 主密钥

主密钥为设备进行加解密和MAC计算的基础密钥，对应附录A中的 2009H数据对象。它不直接用于数据加解密和MAC计算，需要先分解成相应功能的“会话密钥”后再被使用。

* 1. 会话加密密钥

“会话加密密钥”由用“主密钥”对注册数据中的“通信随机码”进行HMAC-SHA256计算得到。用于加解密通信数据。本协议支持最大密钥长度为32字节。

* 1. 会话MAC密钥

“会话MAC密钥”由用“主密钥”对注册数据中的“通信随机码”进行加密结果的前16字节。用于对通信数据进行MAC计算。

1. 交互流程
   1. 常规会话流程

终端先发送“注册请求”（附录A.4），请求中带有表厂商ID，表号信息等数据。主站应答，应答数据中带有时钟信息，终端可用该时钟信息校时。

之后终端上报需要上报的数据对象（附录A）。如果主站有其他操作缓存，则进行交互，交互结束后下发结束帧。开户前使用默认密钥通信。“开户”时，主站要在交互中下发正式密钥。



图5 会话流程

* 1. 记录数据多帧续传流程

记录数据的数据对象（附录A.2）的内容有时因为过大需要分多帧传输，需要使用到多帧续传流程。



图6 多帧续传交互流程

1. （规范性附录）  
   数据对象
   1. 状态数据

状态数据数据上报、读、写格式相同。读请求数据域没有数据。写请求应答2字节错误码（参考表A.8)。是否支持读写在表格中“读写”字段说明。

表A.1.1 状态数据对象

| **ID** | **数据对象名称** | **读写** | **长度** | | **内容** | **加密** | **认证** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0001H | 阀门状态 | RW | 1 | | 对于没有阀门的产品，该数据对象内容为0，且不允许写操作。  阀门状态(0——开阀门；1——关阀门；2——关阀门并锁定） | W | W |
| 0002H | 时钟 | RW | 6 | 1 | 年，BCD码，00H~99H代表2000~2099 | W | W |
| 1 | 月，BCD码，01H~12H代表1月~12月 |
| 1 | 日，BCD码，01H~31H代表1号~31号 |
| 1 | 时，BCD码，01H~23H代表1点~23点 |
| 1 | 分，BCD码，01H~59H代表1分~59分 |
| 1 | 秒，BCD码，01H~59H代表1秒~59秒 |
| 0003H | 当前累计气量 | RW | 4 | | 无符号整数（HEX），数值扩大1000倍用于保留3位小数。 | RW | W |
| 0004H | 主电电压 | R | 2 | | 无符号整数（HEX），电压值扩大1000倍，以保留3位小数，单位V。 | - | - |
| 0005H | 主电电量百分比 | R | 1 | | 无符号整数（HEX）0~100 | - | - |
| 0006H | 备电电压 | R | 2 | | 无符号整数（HEX），电压值扩大1000倍，以保留3位小数，单位V。 | - | - |
| 0007H | 备电电量百分比 | R | 1 | | 无符号整数（HEX）0~100 | - | - |
| 0008H | 预留量 | RW | 4 | | 有符号整数，扩大1000倍以保留3位小数。 | W | W |
| 0009H | 剩余气量 | RW | 4 | | 有符号整数，扩大1000倍以保留3位小数。仅当是气量表时有意义。 | W | W |
| 000AH | 透支状态 | RW | 1 | | 0——非透支；1——透支 | W | - |
| 000BH | 表状态 | R | 2 | | 表A.1.2 | - | - |
| 000CH | 通信随机码 | R | 16 | | 随机数 | - | - |
| 000DH | 单价 | RW | 4 | | 无符号整数（HEX），扩大10000倍以保留4位小数。 | W | W |

表A.1.1 状态数据对象（续）

| **ID** | **数据对象名称** | **读写** | **长度** | **内容** | **加密** | **认证** |
| --- | --- | --- | --- | --- | --- | --- |
| 000EH | 开户状态 | RW | 1 | 无符号整数（HEX）。0-未开户；1-已经开户 | W | W |
| 000FH | 剩余金额 | RW | 4 | 有符号整数（HEX），扩大100倍以保留2位小数。仅当时金额表时有效。 | W | W |
| 0010H | 余量状态 | RW | 1 | 0--余量正常；1--余量不足 | W | W |
| 0011H | NB网络信号强度 | R | 2 | RSRP。有符号整数（HEX） | - | - |
| 2 | SNR。有符号整数（HEX） | - | - |
| 0012H | 通信失败计数 | R | 2 | 无符号整数（HEX）。相邻两次通信成功之间通信失败次数 | - | - |
| 0013H ECL覆盖等级 R 2 有符号整数 (HEX) | ECL覆盖等级 | R | 2 | 有符号整数 (HEX) | - | - |
| 0014H | CellId | R | 6 | BCD码，最多12位，不足高位补0 |  |  |
| 0015H | REAL\_NEARFCN | R | 2 | 实际接入频点,无符号整数（HEX） |  |  |
| 0016H | IMEI | R | 15 | 模组IMEI号 | - | - |
| 0017H | 模组固件版本 | R | 20 | 模组固件版本号，字符串 | - | - |
| 0018H | 模组型号 | R | 10 | 模组型号，字符串 | - | - |
| 0100H | 厂商自定义表状态 | R | 4 | 不同厂商、不同型号的表可以定义不同的内容。这部分内容不在本文档中规定。但同一厂商的相同表型内容定义必须相同。 | - | - |

表A.1.2 表状态

|  |  |  |
| --- | --- | --- |
| **字节** | **BIT** | **说明** |
| BYTE0 | BIT0 | 阀门状态（0：关；1：开） |
| BIT1 | 表具被强制命令关阀（0：否；1：是） |
| BIT2 | 主电电量不足（0：否；1：是） |
| BIT3 | 备电电量不足（0：否；1：是） |
| BIT4 | 无备电，系统不能正常工作（0：否；1：是） |
| BIT5 | 过流（0：否；1：是） |
| BIT6 | 阀门直通（0：否；1：是） |
| BIT7 | 外部报警触发（0：否；1：是） |
| BYTE1 | BIT0 | 计量模块异常（0：否；1：是） |
| BIT1 | 多少天不用气导致阀门关闭（0：否；1：是） |
| BIT2 | 曾出现多天没有远传数据上发成功而导致阀门关闭（0：否；1：是） |
| BIT3 | 电磁干扰（0：否；1：是） |
| BIT4 | （未定义） |
| BIT5 | （未定义） |
| BIT6 | （未定义） |
| BIT7 | （未定义） |

* 1. 记录数据

所有记录数据都是只读的，使用读取记录功能码读取或通过“数据上报”功能码主动上报。

表A.2 记录数据对象

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **数据对象名称** | **方向** | **长度** | **内容** | **加密** | **认证** |
| 1000H | 读时间段事件记录 | ↓ | 2 | 事件代码, FFFFH表示所有类型，其他类型参考表A.7 | - | - |
| 6 | 起始时间，YYMMDDhhmmss, FFFFFFFFFFFFH表示结束时间之前 |
| 6 | 结束时间，YYMMDDhhmmss，FFFFFFFFFFFFH表示起始时间之后 |
| 1 | 记录条数，1字节，应答不超过该条数。FFH表示不限定 |
| ↑ | 1 | 本帧记录条数（1字节）,记为N | - | - |
| N\*11 | 事件记录数据（事件记录格式参考附录A.6） |
| 1001H | 读最新事件记录 | ↓ | 2 | 事件代码, FFFFH表示所有类型，其他类型参考表A.7 | - | - |
| 1 | 记录条数，应答不超过该条数。FFH表示不限定 |
| ↑ | 1 | 本帧记录条数（1字节）,记为N | - | - |
| N\*11 | 事件记录数据（事件记录格式参考附录A.6） |
| 1002H | 读每小时用气日志 | ↓ | 3 | 起始日期，BCD码， YYMMDD | - | - |
| 1 | 天数 |
| ↑ | 3 | 日期，BCD码， YYMMDD | √ | - |
| 1 | 天数 |
| 4\*24\*天数 | 每小时用气数据,无符号整数值扩大1000倍以保留3位小数。 |
| 1003H | 每小时用气上报 | ↑ | 3 | 日期，BCD码， YYMMDD | √ | - |
| 1 | 天数 |
| 4\*24\*天数 | 每小时用气数据,4字节无符号整数（HEX），值扩大1000倍以保留3位小数。 |

表A.2 记录数据对象（续）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **数据对象名称** | **方向** | **长度** | **内容** | **加密** | **认证** |
| 1004H | 读日用气记录 | ↓ | 3 | 起始日期年月日，BCD码， YYMMDD | - | - |
| 1 | 天数 |
| ↑ | 3 | 起始日期年月日，BCD码， YYMMDD | √ | - |
| 1 | 天数 |
| 4\*天数 | 日用气累计量，整数值扩大1000倍以保留3位小数。 |
| 1005H | 日用气记录上报 | ↑ | 3 | 起始日期年月日 YYMMDD | √ | - |
| 1 | 天数 |
| 4\*天数 | 日用气累计量，整数值扩大1000倍以保留3位小数。 |
| 1006H | 读月用气记录 | ↓ | 1 | 年 BCD码 YY | - | - |
| ↑ | 1 | 年 BCD码 YY | √ | - |
| 12\*4  =48 | 月用气累计量，整数值扩大1000倍以保留3位小数 |
| 1007H | 月用气记录上报 | ↑ | 2 | 起始时间 YY | √ | - |
| 12\*4  =48 | 月用气累计量，整数值扩大1000倍以保留3位小数 |

* 1. 设置数据

设置数据数据上报、写请求格式与读应答格式相同。读请求数据域没有数据。写请求应答2字节错误码（参考表A.8)。是否支持读写在表格中“读写”字段说明。

表A.3 设置数据对象

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **数据对象名称** | **读写** | **长度** | **内容** | **加密** | **认证** |
| 2000H | 厂商ID | R | 2 | 无符号整数（HEX） | - | - |
| 2001H | 软件版本 | R | 4 | BCD码 | - | - |
| 2002H | 表型号 | R | 2 | 无符号整数（HEX） | - | - |
| 2003H | 表号参数 | R | 1 | 表号长度，1~32 | - | - |
| 32 | 表号内容，字符串，不足32字节补0 | - | - |
| 2004H | 带阀门 | R | 1 | 0——不带阀门；1——带阀门 | - | - |
| 2005H | 通信模式 | R | 1 | 0，NB-IoT；1，GPRS；2，LoRaWAN；3，红外 | - | - |
| 2006H | 定时上传参数 | RW | 1 | 天数/月份区分位，无符号整数（HEX）。  0：表示按天来发送，例如2天一次，3天一次  1：表示按月来发送，例如每月的2号，每月的3号 | W | W |
| 1 | 无符号整数（HEX）。周期值，如果配置为按天传，则该字段表示几天。如果配置为按月传，则该字段表示每月的几号 |
| 1 | 上传时间，BCD码，表示时。 |
| 1 | 上传时间，BCD码，表示分。 |
| 2007H | 采集服务参数 | RW | 16 | 采集服务地址：字符串，不足16字节补0。 | W | W |
| 2 | 采集服务器端口：无符号整数（HEX） |
| 2008H | 结算方式 | R | 1 | 无符号整数（HEX）0. 金额表；1. 气量表； | - | - |
| 2009H | 密钥参数 | W | 1 | 密钥长度。无符号整数（HEX），1~32 | W | W |
| 1 | 密钥版本 |
| 32 | 密钥 |
| 200AH | SIM卡信息 | R | 20 | 20字节，字符串，对应SIM卡的ICCID | - | - |
| 200BH | 运营商信息 | R | 1 | 0--电信；1--移动；2--联通 | - | - |
| 200CH | 应用协议版本 | R | 2 | BCD码 | - | - |
| 200DH | 供电类型 | R | 1 | 0--碱电；1--锂电 | - | - |
| 200EH | 错峰间隔时间 | RW | 2 | 无符号整数（HEX）。单位秒，范围15~43。 | W | W |
| 200FH | 多天不用气关阀控制参数 | RW | 1 | 无符号整数（HEX）。1字节：0--禁止；1~255 表示天数。 | W | W |
| 2010H | 多天不上传关阀控制参数 | RW | 1 | 无符号整数（HEX）。1字节：0--禁止；1~255表示天数。 | W | W |
| 2011H | 过流报警使能 | RW | 1 | 无符号整数。0：禁止；1：使能 | W | W |
| 2012H | APN | RW | 32 | 字符串。 | W | W |

说明：定时上传错峰方案：定时上传时间 + 表号后3位 ×错峰时间间隔 + 60秒。

* 1. 数据集

数据集数据对象时多种数据对象的集合，相关数据对象的定义参考A.1，A.2，A.3。数据上报、下发、写请求格式与读应答格式相同。读请求数据域没有数据。写请求应答2字节错误码（参考表A.8)。是否支持读写在表格中“读写”字段说明。

表A.4 数据集数据对象

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **数据对象名称** | **读写** | **方向** | **长度** | **内容** | **加密** | **认证** |
| 3001H | 注册请求 | - | ↑ | 6 | 时钟 | - | √ |
| 2 | 厂商ID |
| 2 | 表型号 |
| 33 | 表号参数 |
| 1 | 开户状态 |
| 1 | 运营商信息 |
| 1 | 通信模式 |
| 4 | 软件版本 |
| 2 | 应用协议版本 |
| 16 | 通信随机码 |
| 4 | NB网络信号强度 |
| 1 | ECL覆盖等级 |
| 6 | CellId |
| 2 | REAL\_NEARFCN |
| 15 | IMEI |
| 10 | 模组型号 |
| 20 | 模组固件版本 |
| 1 | 密钥版本 |
| ↓ | 2 | 错误码 |
| 6 | 时钟 |
| 3002H | 通信结束 | - | ↓ | 2 | 错误码 | √ | √ |
| 6 | 时钟 |
| 4 | 剩余气量 |
| 1 | 透支状态 |
| 1 | 余量状态 |
| 4 | 单价 |
| 4 | 剩余金额 |

表A.4 数据集数据对象（续）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **数据对象名称** | **读写** | **方向** | **长度** | **内容** | **加密** | **认证** |
| 3003H | 主动上报数据集 | R | ↑ | 6 | 时钟 | √ | - |
| 1 | 上报方式:0 定时上报；1 手动上报；2 事件上报 |
| 4 | 当前累计气量 |
| 2 | 表状态 |
| 4 | 表厂自定义表状态 |
| 1 | 供电类型 |
| 2 | 主电电池电压 |
| 1 | 主电电量百分比 |
| 100 | 昨天每小时用气日志 |
| 24 | 前5天日用气记录 |

* 1. 用户自定义数据

数据对象ID从A000H~AFFFH为厂商自定义数据对象域。该范围内的数据对象内容由表厂根据指定型号进行定义。不同表厂、型号之间可以不同。但同一厂商的相同表型内容定义必须相同。

* 1. 事件记录格式

事件记录格式：AAAA+YYMMDDHHMMSS+XX；

AAAA:事件类型，2字节，HEX，详见附录A.7；

YYMMDDHHmmSS：事件时间6字节,BCD；

XX预留1字节（用于表示事件详情）；

* 1. 远传表事件记录类型

事件代码2字节，内容参考表A.7。A000H~AFFFH为用户自定义数据记录。

表A.7 远传表事件记录类型

|  |  |
| --- | --- |
| **事件代码** | **事件名称** |
| 0001H | 开阀：执行开阀动作 |
| 0002H | 关阀：执行关阀动作 |
| 0003H | 重新启动 |
| 0004H | 电量低 |
| 0005H | 电量不足 |
| 0006H | 磁干扰 |
| 0007H | 电源断电 |
| 0008H | 异常流量 |
| 0009H | 计量处理单元异常 |
| A000H~AFFFH | 用户自定义事件码 |

* 1. 错误码

表A.8 错误码

|  |  |
| --- | --- |
| **错误码** | **说明** |
| 0 | 无错误 |
| 1 | 数据对象ID不正确 |
| 2 | 日期非法 |
| 3 | 协议代码不支持 |
| 4 | 协议框架版本不支持 |
| 5 | MAC认证错误 |
| 6 | 应用协议版本不支持 |
| 7 | 写参数值非法 |
| 8 | 表号非法 |

1. （资料性附录）  
   校验算法
   1. 校验算法

unsigned short CRC16(unsigned char \*puchMsg, unsigned int usDataLen)

{

unsigned short wCRCin = 0x0000;

unsigned short wCPoly = 0x1021;

unsigned char wChar = 0;

while (usDataLen--)

{

wChar = \*(puchMsg++);

wCRCin ^= (wChar << 8);

for(int i = 0;i < 8;i++)

{

if(wCRCin & 0x8000)

wCRCin = (wCRCin << 1) ^ wCPoly;

else

wCRCin = wCRCin << 1;

}

}

return (wCRCin) ;

}