计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(6):105−109 [doi: 10.15888/j.cnki.csa.006926]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

智能燃气系统中的通信加密方法①

孙建伟[1,2], 樊柯辛[1,2], 张守晨[2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
通讯作者: 樊柯辛, E-mail: fan_kx@126.com

摘　要: 在信息技术快速发展的今天, 物联网技术在各行各业中都得到了广泛的应用, 其中对硬件设备信息的采集以及传输是其主要应用, 但是数据传输过程中会出现严重的数据安全问题, 因此本文提出了一种混合通信加密方法. 本文首先从物联网设备角度出发, 介绍物联网无线通信技术和 CoAP 传输协议以及加密方法, 然后结合物联网设备资源受限制情况, 采用 NB-IoT 技术, 并在智能燃气系统中实现了上述加密方法, 实验以及测试比较的结果表明, 本方法具有可行性.

关键词: NB-IoT; CoAP; 传输协议; 数据加密; 物联网

引用格式: 孙建伟,樊柯辛,张守晨.智能燃气系统中的通信加密方法.计算机系统应用,2019,28(6):105–109. http://www.c-s-a.org.cn/1003-3254/6926.html

Communication Encryption Method in Intelligent Gas System

SUN Jian-Wei[1,2], FAN Ke-Xin[1,2], ZHANG Shou-Chen[2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)

Abstract: With the rapid development of the information technology, the Internet of Things (IoT) technology has been widely used in all walks of life. One of the main applications is the collection and transmission of information from hardware devices. But there will be serious data security problems in the process of data transmission, so the study proposes a hybrid communication encryption method. From the perspective of IoT devices, the study also introduces the wireless communication technology of IoT and the CoAP protocol, and then uses the NB-IoT technology considering the resource constrains of IoT devices, and has implemented the method in smart gas system. The experimental results shows that the proposed method is feasible.

Key words: NB-IoT; CoAP; transmission protocol; data encryption; Internet of Things (IoT)

物联网 (Internet of things), 作为现今信息化时代发展的重要阶段, 指的是实物与实物之间通过互联网相互连接产生联系, 并进行通信和消息的交换, 来实现智能化的应用的一种网络. 现已广泛的应用在工业、医疗、交通、商业、家居、安防报警等领域中[1]. 无论在哪个领域范围内, 物联网的核心关键都是实物与实物之间通过互联网的互联与数据通信.

燃气表与物联网的结合就是利用物联网的数据通信传输能力, 结合数据信息的管理, 实现远程抄表以及空中支付等智能化服务. 在物联网中, 很多终端设备都是资源受限制的, 因此应用层协议选用支持资源受限环境的 CoAP 协议[2]. 本文首先介绍物联网无线通信技术以及加密方法, 然后分析数据传输问题, 提出一种混合通信加密方法, 并应用在智能燃气系统中.

① 收稿时间: 2018-12-12; 修改时间: 2018-12-29; 采用时间: 2019-01-07; csa 在线出版时间: 2019-05-25

© 中国科学院软件研究所 http://www.c-s-a.org.cn

1 相关技术介绍

1.1 NB-IoT 技术简介

窄带物联网 (Narrow Band Internet of Things, NB-IoT), 是对万物互联的物联网设计的一种蜂窝网络连接技术, 顾名思义, 它占用的带宽很窄, 大约只需要 180 KHz, 是 3GPP 推出的标准技术, 是在 LTE 基础上根据自身特点经过修改发展起来的, 使用 License 频段, 其部署方式相对快捷、灵活, 可以使用带内、独立或保护带三种部署场景的方式[3], 不仅能与现有网络并存, 还能直接部署在 GSM、UMTS 或 LTE 网络[4], 即 2/3/4/5G 的网络上, 支持多连接, 实现现有网络的复用，降低部署成本, 实现平滑升级.

1.2 CoAP 协议简介

CoAP(Constrained Application Protocol) 协议, 是专门用于资源受限制型设备或者网络的传输协议, 传输层使用的是 UDP 协议[2,5], 消息开销很小, 消息格式很紧凑, 适用于受处理能力以及功耗的限制的设备网络中. CoAP 协议的设计理念参考了 HTTP 协议, 但是传输的时候有明显的区别, 采用双层结构, 支持异步处理通信和组播[6].

1.3 加密方法简介

数据加密算法大体上分为对称加密算法和非对称加密算法两类. 对称加密算法的加密和解密密钥用的是同一个, 故速率快, 适用于大数据量, 但是安全性不高. 非对称加密算法有两个密钥, 分为公钥和私钥, 一个作为加密密钥, 一个作为解密密钥, 故安全性高, 但是算法复杂, 速率慢, 因此用的时候时常将对称加密算法和非对称加密算法混合起来一起使用.

2 物联网通信技术及加密算法的研究

2.1 物联网无线通信技术的研究

物联网中的无线通信技术主要分为两类, 短距离的无线通信技术有 ZigBee、Wi-Fi、蓝牙等[5], 另一类是 LPWAN(low-powerWide-AreaNetwork), 也就是广域网通信技术, 它又包括工作在未授权频谱下的 LoRa 技术和工作在授权频谱下的 NB-IoT 技术[7], 这些技术的基本性能比较, 如表 1 所示.

通过比较可以发现, LoRa 技术和 NB-IoT 技术都可用于远距离通信, 但是 LoRa 工作在未授权频谱下, NB-IoT 技术工作在授权频段下, 干扰相对少一些, 并且可以与现有的蜂窝网络融合并存, 易于快速大规模的部署, 更适用于智能燃气系统.

表 1 物联网常用无线通信方式比较

方式	通信距离	传输速度	功耗 (mA)	安全性	成本 ($)
ZigBee	10–75 m	<250 Kbps	5	中等	6
Wi-Fi	<100 m	11–54 Mbps	10–50	低	25
蓝牙	<100 m	1 Mbps	20	高	5
LoRa	<10 km	0.3–50 Kbps	5	高	6
NB-IoT	<15 km	65 Kbps	5	高	5–10

2.2 加密算法的研究

混合加密算法常用的有 DES_RSA[8]算法, 使用 DES 算法对明文数据进行对称加密, 再使用 RSA 算法对对称加密的密钥进行非对称加密, 在提高安全性的同时, 不降低加密速度, 且这样做也适用于大量数据的加密. 这些混合加密算法大多是针对非物联网的应用环境下, 针对物联网环境更倾向于选择轻量级加密算法, 即在算法的强度符合安全需求的情况下, 对终端的资源消耗也不大, 这样更符合物联网环境.

由于燃气表设备资源受限, 本文选取轻量级加密算法 RC4 算法, 它不仅对资源消耗小, 而且加解密速度快, 为了安全性考虑, 结合 DH 算法配合使用, DH 算法负责计算并交换密钥, RC4 算法负责对数据进行加密, 在保证加密速度的同时提高安全性.

3 系统实现

基于本文提出的技术, 以智能燃气系统为背景, 设计了通信协议和加密方法, 系统总架构如图 1 所示.

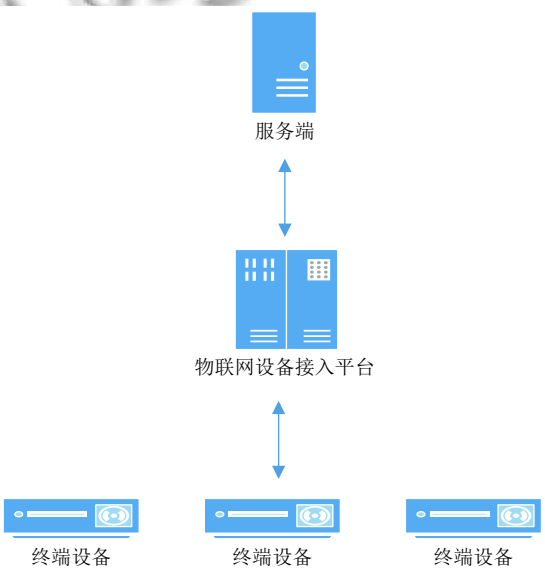

图 1 系统架构图

© 中国科学院软件研究所 http://www.c-s-a.org.cn

系统由终端设备网络、物联网设备接入平台、服务端三个部分组成.

3.1 通信协议设计

本系统中设备受到处理能力和功耗等因素的限制, 无法使用 TCP 或者 HTTP 等复杂的应用层协议进行数据的传输, 因此选用 CoAP 协议, 根据其结构, 将数据传输通信协议在 CoAP 协议的 payload 上进行扩展定义, 传输的格式使用解析方便的 JSON 格式, 传输运行在 UDP 协议上.

3.2 加密算法设计

RC4[9]加密算法是 Ron Rivest 提出来的密钥长度可变的流加密算法簇, 以字节流的形式依次对数据中的一个个的字节进行加密, 解密的时候亦然. 它的加解密速度很快, 核心思想是产生一种被叫做密钥流的伪随机流, 之后进行加密和解密步骤, RC4 算法的具体描述如下, 原理如图 2 所示.

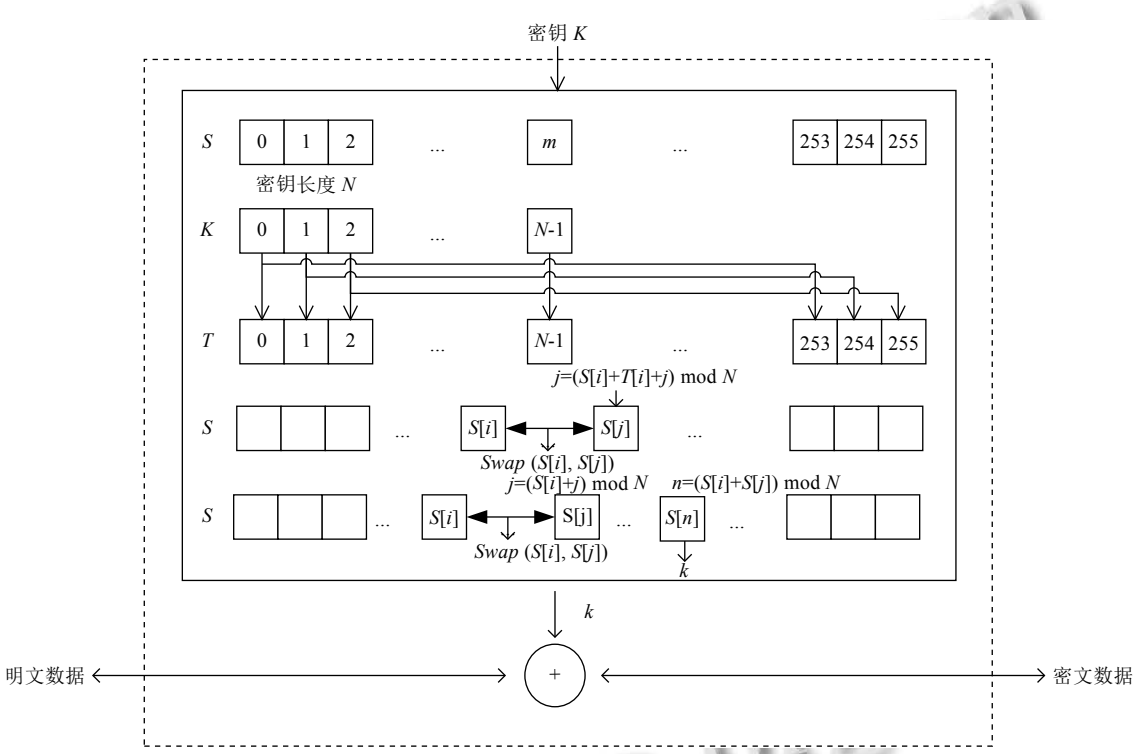

图 2 RC4 算法原理图

(1) 取一个密钥 K, 使用 KSA (Key Sheduling Algorithm) 密钥调度算法对状态向量 S 也就是 S-box 进行初始化和替换, 首先通过密钥 K 得到向量 T, 根据 $S[i]$和 $T[i]$的值与随机取的 j 值进行取余得到新的 j 值并交换, 目的是将 S-box 的元素都处理并随机置换;

(2) 将上一步得到的 S-box 值使用 PRGA (Pseudo Random Generation Algorithm) 伪随机生成算法生成得到密钥流 k, 取一个位置 i 的值, 通过相加取余的方式得到另一个位置 j 的值, 之后交换并相加取余得到新的位置 t 的值即为密钥流 k 的元素之一, 循环执行这个操作即可得到完整密钥流 k;

(3) 将明文数据与密钥流 k 进行 xor 操作就是加密的过程, 将密文数据与密钥流 k 进行 xor 操作就是解密过程.

Diffie-Hellman 算法[10]简称 DH 算法, 是一种基于非对称加密的动态密钥交换算法, 这个算法也是使用公钥和私钥的形式, 但是双方交换公钥信息之后可以产生一个共享的一致的密钥, 这个密钥就可以作为后续操作中的加密算法的密钥, 其原理如图 3 所示, 具体描述如下:

(1) 选取一个素数 p 和整数 q, q 是 p 的一个原根, 并且 q 的值要小于素数 p 的值, 这两个数的值公开;

(2) Anne 选取一个私钥 l, 值小于素数 p 的值, 计算得到公钥$K_a = q^l \mod p$, 并发送给 Bill;

(3) Bill 选取一个私钥 r, 值小于素数 p 的值, 计算得到公钥$K_b = q^r \mod p$, 并发送给 Anne;

© 中国科学院软件研究所 http://www.c-s-a.org.cn

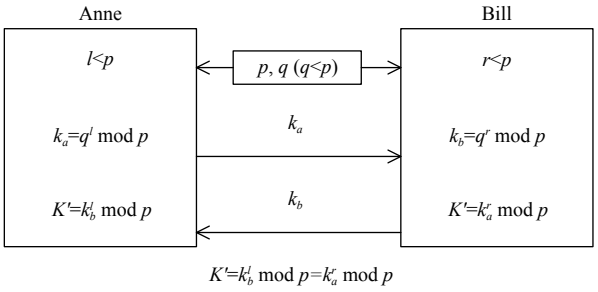

图 3 DH 算法原理图

(4) Anne 和 Bill 双方各自根据对方的公钥和自己的私钥计算得到共享密钥$K' = k_b{}^l \bmod p = k_a{}^r \bmod p$.

本文中数据传输的加密算法选择 RC4 算法和 DH 算法结合使用, 由于 DH 算法存在中间人攻击的漏洞, 也就是中间人会冒充通信双方来通信并获取公钥信息自行计算获得共享密钥, 所以本系统中会加密传输 DH 算法中的公开变量以及公钥等信息, 具体流程如图 4 所示, 步骤如下:

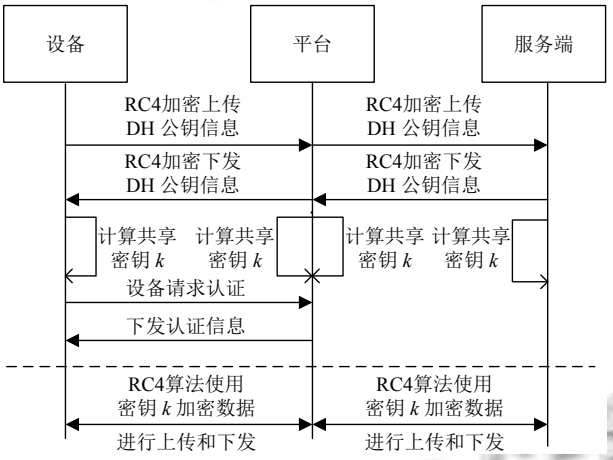

图 4 数据传输流程图

(1) 设备端使用 RC4 算法固定密钥传输 DH 算法中的公开变量以及公钥信息, 避免中间人攻击获取共享密钥.

(2) 平台端收到设备端公钥并验证之后, 加密传输自己的公钥给设备端.

(3) 设备端和平台端分别都根据自己得到的对方的公钥和自己的私钥计算得到共享密钥.

(4) 平台与服务端获取共享密钥的过程和设备端与平台之间的过程一样.

(5) 设备进行身份认证并获取认证信息, 成功之后进入数据加密传输阶段.

(6) 设备端根据计算得到的共享密钥使用 RC4 算法对传输的数据进行加密之后传输到平台.

(7) 平台端根据计算得到的共享密钥使用 RC4 算法对数据进行加密, 然后传输到服务端.

4 实验分析

本文实现了以窄带物联网的通信技术为基础的通信协议的设计以及加密的方案, 应用在智能燃气系统上, 以实现燃气数据自动实时的采集以及传输, 便于燃气公司实现远程抄表等功能, 以及对居民用户燃气用量的智能管理等操作.

本文中设备端使用的设备还是以传统的燃气表为基础设施, 外加 STM8L052R8 型号处理器并内置光电直读技术以及 NB 模组, 平台使用物联网集成管理平台, 服务端使用阿里云服务进行部署.

通过抓包工具抓取到的数据传输通信协议包如图 5 所示, 可以看到数据传输运行在 UDP 协议之上, 并加密进行通信, 传输到服务端之后经过可视化处理, 显示在管理系统上, 系统中燃气表的数据如图 6 所示, 对数据传输的加密方法做的测试比较如表 2 所示.

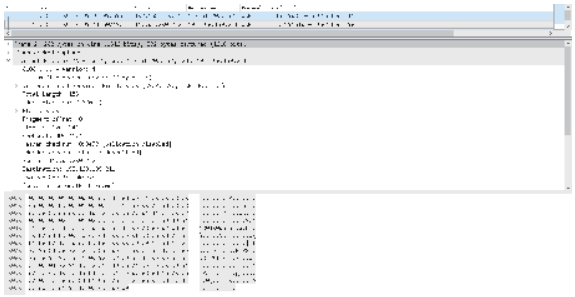

图 5 数据传输协议包图

图 6 系统中燃气表数据图

本文数据加密方法中 DH 算法的作用是计算共享密钥, 数据的加密主要还是靠对称加密算法来做, 所以这里只比较了常用的对称加密算法 DES 和 RC4 的一

© 中国科学院软件研究所 http://www.c-s-a.org.cn

些性能. 由于 DES 加密算法的密钥长度是 64 位[8], 所以表中比较了该密钥长度下的明文数据量变化的情况, 从表中可以看出随着明文数据量的增加该算法的空间资源的大小发生了一些变化, 时间也随之增加. 由于 RC4 算法的密钥长度是可变的, 在表中分别比较了 64 位和 128 位情况下随着数据量增加的情况, 可以看出其空间资源的大小也发生了一些变化, 时间同样随着数据量的增加而上升, 但是在同等条件下与 DES 算法相比, 速度明显比 DES 算法快, 空间资源的占用也比其小, 另外, RC4 的密钥长度是可以变化的, 当密钥长度足够长的时候它的安全性也越高, 所以 RC4 算法在本系统中的应用更具有优越性.

表 2 加密方法测试比较

	密钥长度 (bit)	明文长度 (bit)	存储空间 Flash(KB)	运行空间 SRAM(KB)	时间 (ms)
DES	64	64	3.07	3.86	10.2965
		128	3.18	3.86	10.2991
		256	3.19	3.86	10.3004
		512	3.23	3.86	10.3028
RC4	64	64	1.23	1.62	0.9433
		128	1.23	1.63	0.9737
		256	1.25	1.64	1.0345
		512	1.28	1.67	1.1561
	128	64	1.23	1.63	0.9289
		128	1.24	1.63	0.9593
		256	1.26	1.65	1.0201
		512	1.29	1.68	1.1417

5 结论与展望

物联网中通信技术的不断更新使得数据传输在能够正常通信的基础上考虑到安全性的问题. 本文通过对窄带物联网通信技术以及 CoAP 传输协议的研究, 并结合实际应用场景, 提出一种混合通信加密方案, 目的是为解决在物联网设备资源受限制情况下的设备端与服务端的通信以及安全传输的问题, 经过实现和测试, 验证了这个方案能够解决上述问题, 其安全性以及增加的时间成本的开销也都在可以接受的范围内.

在目前的工作中已经验证了该方案的可行性, 在后期的工作中还会考虑其普适性问题, 进一步的完善该方案.

参考文献

1 苏世旭. 面向居家服各环境的智能信息系统数据处理模块设计与实现[硕士学位论文]. 南京: 南京邮电大学, 2017.

2 Bormann C, Castellani AP, Shelby Z. Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Computing, 2012, 16(2): 62–67. [doi: 10.1109/MIC.2012.29.]

3 陈发堂, 邢苹苹, 杨艳娟. 窄带蜂窝物联网终端上行资源调度的分析与设计. 计算机应用, 2018, 38(11): 3270–3274, 3281. [doi: 10.11772/j.issn.1001-9081.2018040849]

4 Zayas AD, Merino P. The 3GPP NB-IoT system architecture for the Internet of Things. Proceedings of 2017 IEEE International Conference on Communications Workshops. Paris, France. 2017. 277–282. [doi: 10.1109/ICCW.2017.7962670]

5 徐召杰. 物联网中基于双向认证的安全通信协议的研究与实现[硕士学位论文]. 北京: 北京邮电大学, 2018.

6 陈旖, 张美平, 许力. WSN 应用层协议 MQTT-SN 与 CoAP 的剖析与改进. 计算机系统应用, 2015, 24(2): 229–234. [doi: 10.3969/j.issn.1003-3254.2015.02.043]

7 Sinha RS, Wei YQ, Hwang SH. A survey on LPWA technology: LoRa and NB-IoT. ICT Express, 2017, 3(1): 14–21. [doi: 10.1016/j.icte.2017.03.004]

8 陈侨川. 一种基于 DES 和 RSA 算法的混合加密算法[硕士学位论文]. 昆明: 云南大学, 2015.

9 苗三立, 左金印, 宋宇飞. 基于 FPGA 的 RC4 加密算法设计及实现. 计算机测量与控制, 2018, 26(2): 252–254, 263. [doi: 10.16526/j.cnki.11-4762/tp.2018.02.062]

10 才大壮, 杨海波. 使用两阶段 DH 算法的 IMS 接入侧安全通信模型研究. 小型微型计算机系统, 2016, 37(4): 782–786. [doi: 10.3969/j.issn.1000-1220.2016.04.027]

© 中国科学院软件研究所 http://www.c-s-a.org.cn