基于CLA和TLS结合实现的物联网通信安全研究

Research on Communication Security of IoT Based on CLA and TLS

张晓辉[1]，王首媛[2]，慕江林[1]（1. 中讯邮电咨询设计院有限公司成都分公司，四川 成都 610000；2. 中讯邮电咨询设计院有限公司，北京 100048）

Zhang Xiaohui[1], Wang Shouyuan[2], Mu Jianglin[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd. Chengdu Branch, Chengdu 610000, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China）

摘　要：

提出了一种结合CLA无证书认证技术和TLS安全传输协议的物联网设备认证和通信机制，该机制使用无证书密码系统为物联网设备签发数字身份，结合无证书TLS协议实现设备之间的认证和加密通信。相对传统CA证书认证机制和基于标识的公钥密码体制，本机制在保证物联网设备之间安全通信的情况下，有效降低了CA体制中设备身份认证的证书传输成本，同时解决了标识认证体制中的密钥托管等问题。

关键词：

物联网；CLA；TLS；无证书认证技术

doi：10.12045/j.issn.1007-3043.2021.07.006

文章编号：1007-3043（2021）07-0024-03

中图分类号：TN929.5

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

It proposes an IoT device authentication and communication mechanism, which combines CLA certificateless authentication technology and TLS secure transmission protocol. This mechanism uses a certificateless authentication system to issue digital identities for IoT devices, and combines certificateless TLS protocol to achieve authentication between devices and encrypted communication. Compared with the traditional CA certificate authentication mechanism, this mechanism effectively reduces the certificate transmission cost in the device authentication process and solves the key escrow problem in identity authentication system while ensuring the secure communication between IoT devices.

Keywords：

IoT; CLA; TLS; Certificate-free authentication technology

引用格式：张晓辉，王首媛，慕江林. 基于CLA和TLS结合实现的物联网通信安全研究[J]. 邮电设计技术，2021（7）：24-26.

1 概述

物联网有着无数的终端设备、复杂的信息通信渠道、庞大的数据存储与处理中心。相对于互联网，物联网的终端有可移动化、微型化、海量化的特征，其传输通道涉及有线网络和无线网络，物联网的体系结构中呈现出可编程、可通信、智能化、网络化的特点，因此物联网面临特殊的安全挑战[1]。

本文基于CLA无证书密码技术和TLS传输层安全协议，提出物联网设备认证和安全通信技术方案。该方案重点解决物联网通信过程中设备身份认证困难和数字证书传输成本过高等问题。

该方案采用CLA无证书密码技术为物联网设备生成数字身份，将CLA无证书认证技术集成到TLS传输层安全协议，基于国密SM2、SM3和SM4算法，形成CLA无证书密码套件。采用TLS握手过程进行设备身份认证和密钥协商，物联网设备通过TLS加密通道进行安全通信。

收稿日期：2021-06-01

2 物联网通信安全现状

2.1 物联网身份认证现状

当前物联网大多采用传统的PKI/CA证书体制，采

用X.509证书格式，在IoT物联网平台注册私有CA证书，在设备侧绑定设备证书，通过TLS中的RSA算法套件等进行设备认证和通信。

部分物联网设备采用基于标识的认证体制，例如部署基于国密SM9的基础密码设施，在应用层部署SM9密钥中心，在设备侧部署SM9私钥。通过SM9数字签名算法实现设备认证。

2.2 现有物联网身份认证存在的问题

基于数字证书的PKI/CA是目前广泛使用的公钥密码体制，由可信的证书权威机构（CA）为每个用户签发一个公钥证书。公钥证书包括了用户的身份信息、用户的公钥和CA的签名。在PKI/CA中，证书的格式一般采用X.509格式，这种格式的证书一般具有1~2 KB的数据长度。在证书中至少应包含用户名称、CA名称、证书有效期、用户公钥、CA对上述信息的签名等几项内容。

物联网中使用PKI/CA体制具有如下缺点。

a）CA证书字节数过多，证书在传输和存储的过程中需要占用大量的网络带宽和存储资源，不适合存储空间和网络宽带受限的物联网设备。

b）CA证书管理复杂，对于海量物联网设备，证书的颁发、存储和撤销等过程开销巨大。

对于使用标识认证的物联网设备，由于存在密钥托管问题，用户签名不具有唯一性和不可否认性，另外还存在密钥撤销更换困难等问题。

3 TLS安全传输层协议

TLS协议由握手协议、更改密码规范协议、警告协议和记录协议组成[3]。其中握手协议的目的是建立安全的数据传输信道，更改密码规范协议规定了更改密码规范的具体标准，警告协议规定了协议如何处理通信错误的情况，记录协议用于进行数据传输。

TLS通信过程如图1所示。

TLS协议能够提供认证、机密性、完整性、重放保护等安全功能，是应用最广泛的安全通信协议。当前互联网和物联网都广泛采用CA搭配TLS协议进行身份认证和加密通信。

4 基于CLA的无证书认证技术

在CLA无证书公钥密码体制中，由于用户密钥是由用户和KGC共同生成的，所以不存在密钥托管问题，能够保证用户签名的唯一性和不可否认性。

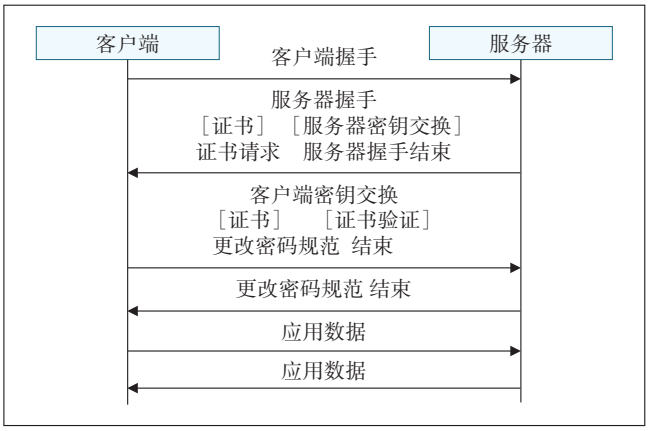

图1 TLS通信

以256 bit的CLA的无证书密码体制为例，在用户标识不超过32 B时，签名与用户标识及部分公钥的总长度不超过128 B，远小于1~2 KB的CA证书，能够有效降低存储空间和传输带宽需求。

CLA无证书密码技术可以采用国密SM2椭圆曲线参数，使用国密标准定义的数字签名算法进行身份认证。

5 CLA和TLS结合的物联网安全通信

5.1 基于CLA的物联网设备管控系统

基于CLA的物联网设备管控系统作为物联网设备的身份管理中心，负责审核实体合法性，为物联网设备提供无证书公钥密码体制的密钥及密钥标识生成、密钥及密钥标识管理、密钥标识发布和密钥状态管理，提供密钥生存周期全过程的安全管理和维护。主要功能如图2所示。

a）物联网身份管理系统（IDM）。物联网身份管理系统主要负责审核物联网设备身份的合法性，维护物联网实体身份状态，提供注册、挂失、注销和恢复等服务。

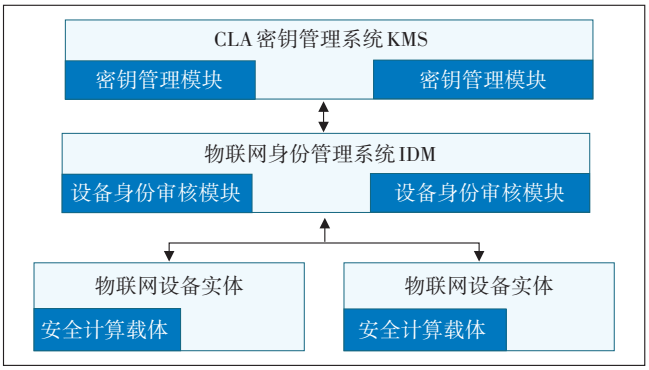

图2 无证书物联网设备管控系统组成结构图

b）CLA密钥管理系统（KMS）。密钥管理系统负责生成和保存系统主密钥，负责利用CLA密钥算法为物联网设备生成部分密钥。

c）物联网设备实体。物联网设备实体可以是网络上的服务器、打印机、路由器、网卡、个人计算机、移动终端、货物和商品等。实体的密钥载体可以为带SM2算法的密码机、密码卡、PSAM卡、TF卡（SD卡）、电子标签或云密码等。

5.2 基于CLA的无证书TLS协议

在无证书公钥密码体制中，公钥被分成2个部分，一部分由设备自己生成，另一部分由系统公钥从用户ID导出。在计算设备实际公钥时，实际上是对系统私钥签名的验证，自动隐含了对设备公钥的认证。

在TLS通信协议中集成CLA无证书认证，主要改造在握手协议阶段。按照国密标准，签名验签和加密解密使用2组密钥。使用国密SM2算法进行签名验签、加密解密，在TLS中进行身份认证和密钥交换；使用国密SM4算法作为对称加密算法，在TLS中构造加密通信隧道；使用国密SM3算法作为消息验证的MAC算法，保障TLS信息完整性；形成基于国密SM2的CLA-SM4-SM3加密套件。TLS无证书认证过程如下。

a）客户端使用签名私钥对数据进行签名，拼接客户端公钥标识，发送ClientHello消息给服务端。

b）服务端使用系统CLA公钥和客户端公钥标识计算客户端实际公钥，使用实际公钥验证客户端签名，验证通过则说明客户端身份合法。

c）服务端使用签名私钥对数据进行签名，拼接服务端公钥标识，发送ServerHello消息给端客户。

d）客户端使用系统CLA公钥和服务端公钥标识计算服务端实际公钥，使用实际公钥验证服务端签名，验证通过则说明服务端身份合法。

e）双向身份认证通过，进行消息加密通信。

通过在TLS握手认证阶段集成CLA无证书认证技术，实现了物联网设备通信时的双向设备身份认证，同时保障了设备间通信的安全性和不可否认性。

5.3 基于CLA无证书密码体制与TLS安全传输协议的物联网通信

通过无证书物联网设备管控平台和无证书TLS协议，物联网设备间可以进行身份认证和加密通信，设备初始化及通信过程如图3所示。

a）物联网设备生成设备公私钥，提交设备相关信息和公钥信息到无证书物联网设备管控平台申请设备注册。

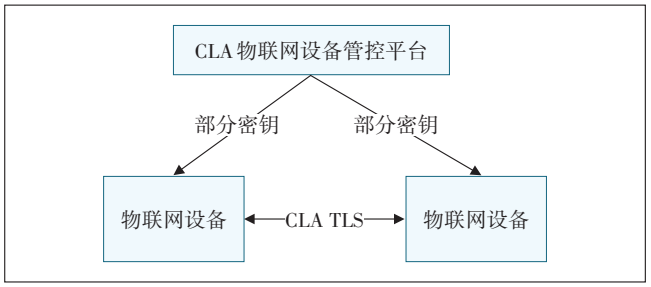

图3 无证书物联网设备管控与无证书TLS通信

b）平台验证物联网设备合法性，通过后将通过系统密钥和设备公钥利用CLA算法生成部分公私钥，用数字密码信封保护发送给设备。

c）物联网设备使用自身密钥和密码信封内容生成设备数字身份信息，设备初始化过程完成。

d）设备和设备之间通过无证书TLS协议进行通信。在TLS握手过程中进行设备的双向认证，若认证通过则进行消息加密通信，认证失败则断开连接。

6 结束语

将CLA无证书密码技术和无证书TLS传输协议结合，替换传统CA和TLS传输协议架构，在保障物联网安全的前提下实现了物联网的高效通信。物联网设备对私钥具有完全自主权，对公钥具有自证性；签名具有不可否认性并可即时验证；密钥可撤销和更换；能够适应大型复杂、用户数量众多且分布广泛的物联网环境，降低了物联网通信的负载和设备的能耗。综上，该方案应用在物联网安全通信领域优势明显。

参考文献：

[1] 杨婷，张光华，刘玲，等. 物联网认证协议综述[J]. 密码学报，2020，7(1)：87-101.

[2] 武传坤，王九如，崔沂峰. 物联网的OT安全技术探讨[J]. 密码学报，2020，7(1)：134-144.

[3] 毕兴，唐朝京. 基于模型检测的TLS协议实现库安全性分析[J]. 系统工程与电子技术，2021，43(3)：8.

[4] 熊荣华. 一种无双线性对运算的无证书公钥密码体制的实现方法：CN104539423.3[P]. 2015-04-22.

作者简介：

张晓辉，毕业于山东大学，工程师，主要从事安全产品研发工作；王首媛，毕业于北京邮电大学，IT研发BU总监，硕士，主要从事物联网安全、密码应用研究、产品规划设计、产品生命周期管理等工作；慕江林，毕业于西华大学，工程师，硕士，主要从事安全产品研发工作。