文章编号:1671-4598(2024)10-0208-07 DOI:10.16526/j.cnki.11-4762/tp.2024.10.030 中图分类号:TP271.5 文献标识码:A

基于 E2000D 的工业物联数采安全终端研究与设计

靖琦东，蒋增文，田 炜，万里云，周秩辉
（中电工业互联网有限公司，长沙 410000）

摘要：工业物联网的出现使工业数据安全备受关注，数据采集的安全直接关系到了工业互联网的数据安全；数据采集系统中，数据采集（南向）和云端通信（北向）协议及数据采集系统运行环境是数采终端最主要的安全攻击目标；在对工业物联数采安全终端主流北向 MQTT 协议和南向 OPC UA 协议的安全性及数采系统可信运行环境进行分析后，在国产处理器 E2000D 安全可信运行环境上基于 OpenSSL 库设计并实现了支持北向 MQTT 和南向 OPC UA 协议的工业数采安全终端；通过试验测试表明，该工业物联数采安全终端在安全认证、访问控制、数据完整性和数据机密性方面都有较高的安全性能。

关键词：工业物联网；E2000D；OPCUA；OpenSSL；数采安全终端

Research and Design of Industrial IoT Data Acquisition Security Terminal Based on E2000D

JING Qidong, JIANG Zengwen, TIAN Wei, WAN Liyun, ZHOU Zhihui
(Internet Co., Ltd. of CEC Industry, Changsha 410000, China)

Abstract: The emergence of Industrial Internet of Things (IoT) has paid attention to industrial data security. The security of data collection is directly related to the data security of the industrial Internet. In the data acquisition system, the data acquisition (southbound) and cloud communication (northbound) protocols and the operating environment of the data acquisition system are the most important security attack targets of data acquisition terminals. This paper analyzes the security of the mainstream northbound message queuing telemetry transport (MQTT) protocol and southbound object linking and embedding (OLE) for process control unified architecture (OPC UA) protocol of the industrial IoT data mining security terminal and the trusted operating environment of the data acquisition system, designs and implements a data mining security terminal supporting northbound MQTT and southbound OPC UA protocol based on OpenSSL library in the secure operating environment of domestic processor E2000D. Experimental results show that the industrial IoT data acquisition security terminal has a high security performance in security authentication, access control, data integrity and data confidentiality.

Keywords: Industrial IoT; E2000D; OPC UA; OpenSSL; data acquisition security terminal

0 引言

工业互联网的出现打破了工业系统的封闭环境，工业体系逐步由封闭走向开放，工控安全成为工业网联系统关注的焦点。当前工业互联网的安全保障开始从外围防护向内生安全，从被动防护向主动感知转变[1]。

工业物联网终端是实现工业数据采集的核心设备，终端安全关乎工业互联网的内生安全[2-3]。2019 年国家发布的信息安全等级保护标准[4]提出了对物联网感知节点物理防护及设备本体安全等四方面的新要求。

文献［5］在研究泛在物联网终端设备安全威胁时指出终端软件漏洞、网络通信安全和数据泄漏是物联网终端的典型安全威胁。工业物联网终端要实现数据互联主要涉及南向协议（连接设备）、北向协议（连接云平台）和终端安全可信运行环境等几个主要方面，这几个方面也是工业物联网终端数据泄露的关键点。

在北向协议方面，消息队列遥测传输（MQTT，message queuing telemetry transport）协议因其轻量级、易用、可连接大量远程传感器的控制设备而成为当前使用最多的云端通信协议[6]。但据从 SHODAN 搜索的数据显示，MQTT 作为物联网终端连接云服务器主流的物联网协议，仅有不到 1%的终端使用了安全方式传输。协议存在较为严重的数据泄漏等安全风险。

收稿日期:2023-09-22； **修回日期**:2023-11-02。
基金项目:湖南省创新型省份建设专项[高新技术产业科技创新引领计划](2021GK4012)。
作者简介:靖琦东(1974-),男,硕士,高级工程师。
通讯作者:蒋增文(1984-),男,硕士研究生,工程师。
引用格式:靖琦东,蒋增文,田 炜,等.基于 E2000D 的工业物联数采安全终端研究与设计[J].计算机测量与控制,2024,32(10):208-214,221.

在南向协议方面，OPC 统一架构（OPC UA，OLE for process control unified architecture）是由 OPC 发展而来的，用于解决当前工业自动化领域存在的兼容性、开放性、通用性问题的统一标准通信接口[7-8]。作为工业 4.0 时代的核心通信接口规范[9]，在工业设备与自动化的数据采集与控制中逐渐得到了广泛的应用。OPC UA 的通信基于工业以太网，在复杂的工业网联系统中数据很容易被暴露，为此通信安全也不容忽视。

在物联网终端硬件平台方面，当前终端主要以国外处理器构成的平台为主，包括 ST、TI、NXP、Intel 等，国产平台较为少见。但在“芯片禁令”等复杂国际形势下，硬件平台安全导致终端运行的环境并不可信，也是工业物联数采终端安全主要的威胁。

基于国产化 Phytium E2000D 硬件平台，从终端自身安全角度对 MQTT 和 OPC UA 的安全进行研究，从可信安全环境、南向协议（OPC UA）、北向协议（MQTT）3 方面着手，设计和实现一种基于国产平台的工业物联数据采集安全终端，解决工业物联网数据采集终端的安全问题。

1　终端安全策略

1.1　数据加解密

信息安全通常包括保密性、完整性和可用性 3 个部分。

采用数字签名的方式对信息摘要进行签名，以保证传输的完整性，防止传输过程中被恶意篡改。主流的数字签名算法有 MD5、SHA1、SHA256、SHA1WithRSA 等。

对消息内容的加解密是实现保密性的重要手段，传输内容通过加密将明文转换成密文，保证传输内容的安全性。加密算法分对称加密和非对称加密两种[10]，对称加密的加解密采用同一个密钥。AES[11-12]是目前效率最高，安全最优的分组加密算法，密钥长度有 128、192 和 256 位共 3 种，常用于对消息体的加解密。其缺点在于密钥管理和传输存在一定的泄密风险。

AES 的加密和解密采用同一套密钥，通常需要通过非对称加密算法对密钥进行加密后再进行传输，以防止密钥泄密。设明文为 P，密钥为 K，密文为 C，设加密函数为 E，则加密公式为：

$$C = E(P,K) \tag{1}$$

若设解密函数为 D，则有解密公式为：

$$P = D(C,K) \tag{2}$$

在算法实现时，AES 将明文序列 P 进行分组，进行轮密钥加、字节代换、行位移和列混合后输出密文 C。列混合变换通过矩阵相乘来实现，经行移位后的状态矩阵与固定矩阵相乘得到混合后的状态矩阵。解密时，将密文 C 进行逆行位移、逆字节代换、轮密钥加后输出明文 P。加解密流程如图 1 所示。

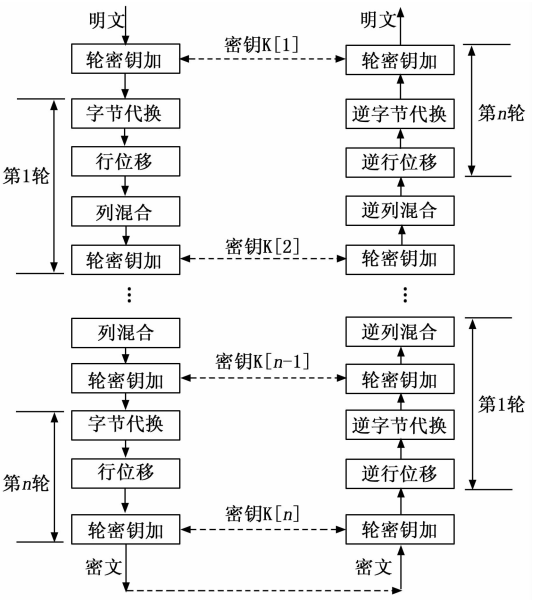

图 1　AES 加解密流程

非对称加密是一种使用公钥和私钥配对的加密方法，其解决了对称加密中密钥配送不安全的问题。非对称加密采用公钥分发，私钥保密规则。公钥公开，可以自由分发传递，而私钥是保密的，只有私钥持有者才拥有。非对称加密算法主要有两种方式：一种是公钥加密，私钥解密，另一种则是私钥签名，公钥验签。

常见的非对称加密算法包括 RSA、DSA 等。RSA[13]是当前最为流行和成熟的非对称加密算法，采用公私钥一对密钥机制，解决了密钥传输涉密的问题。常用于密钥传输、数字签名与验签。密钥长度通常有 512 位，1 024 位，2 048 位等。RSA 的最大的缺点在于加密效率低。RSA 算法实现通常由公钥私钥生成、RSA 加密和 RSA 解密 3 步组成。

设两个由 k 位组成的素数 p 和 q，k 的取值越大，密码越难破解。设 n 为 p 和 q 的乘积，令：

$$\varphi(n) = (p-1)(q-1) \tag{3}$$

任选整数 e，满足：

$$\begin{cases} \gcd[e,\varphi(n)] = 1 \\ 1 < e < \varphi(n) \end{cases} \tag{4}$$

其中：$\gcd[e,\varphi(n)]$ 表示 e 和 $\varphi(n)$ 的最大公约数，当最大公约数为 1 时称为互素。那么 e 称为加密钥，也称公钥，通常表示为 (n,e)。

设整数 d 满足：

$$\begin{cases} de \bmod \varphi(n) = 1 \\ de = b\varphi(n) + 1, b \geqslant 1 \text{ 且为整数} \end{cases} \tag{5}$$

其中：mod 表示取模。d 称为 e 在 $\varphi(n)$ 域上的逆元，即解密钥，表示为 (n,d)，解密钥为私钥，由解密方持有，不对外公开。

设 x 为明文，y 为密文，则通过公钥 (n,e) 加密的公式表示为：

$$y = x^e \bmod n \tag{6}$$

通过私钥 (n,d) 的解密公式为：

$$x = y^d \bmod n \tag{7}$$

数字证书是通信双方标识身份信息的一系列数据，通常由一个 CA 机构签发。证书中存入公钥、用户信息、CA

机构信息和数字签名的文件，用于双方身份认证。X.509 是密码学里公钥证书的格式标准，在 SSL/TLS 及其它很多非在线场景中有广泛的应用。X.509 证书里包含了公钥、身份信息和签名信息。

1.2 身份认证

安全套接层（SSL，secure sockets layer）协议是一种国际标准的加密及身份认证通信协议，在传输层与应用层之间对网络连接进行加密。SSL 协议向基于 TCP/IP 的通信双方提供鉴别、数据完整性和机密性的安全保障。

数据正式交换前，通过握手交换 SSL 身份信息，实现互相认证以达到安全特性审查的目的。在交换密钥和身份信息时，使用数字签名确保完整性、使用加密确保私密性。SSL 协议已成为事实上的工业标准，在 Internet 的服务器与客户端中已得到了广泛的使用[14]。

SSL 协议可以提供数据加密、数字签名和安全连接等功能。SSL 协议可分为 SSL 记录协议层和 SSL 握手协议层[15]。SSL 记录协议层位于传输层之上，为应用层提供数据封装、压缩、加密等服务。SSL 握手协议层建立在 SSL 记录协议层之上，是 SSL 的核心部分。SSL 协议层包含了握手协议、密码修改协议和报警协议，主要用来实现各种算法协商、服务器认证、客户端认证和密钥生成。

SSL 支持证书、对称加密码、非对称加密、摘要消息签名等多种密码算法。SSL 在建立安全通道前需要进行证书交换和加密算法的协商。在建立了认证和协商后才根据数字签名保证信息的完整性，通过对称加密算法对保证数据的安全，通过非对称加密码算法对密钥进行保护。

2 终端设计与实现

2.1 终端总体设计

基于 E2000D 的工业物联数采安全终端由 E2000D 可信环境和 E2000D 数采软件两部分组成。如图 2 所示。

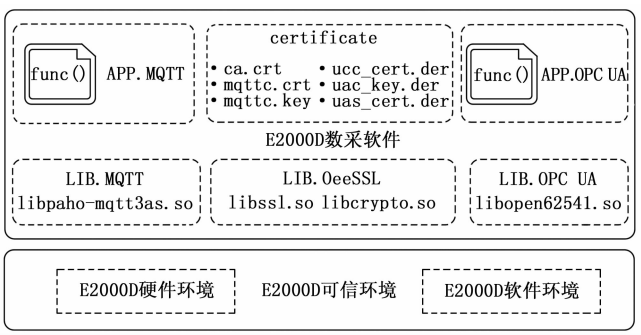

图 2 数采安全终端总体框图

E2000D 可信环境为数采终端的运行提供安全支撑环境，由硬件环境和软件环境两部分组成。硬件环境由国产自主可控处理器 E2000D、国产以太网芯片裕太微 YT8521SH 等自主可控芯片构成。软件环境遵循飞腾安全处理器平台架构规范（PSPA，phytium security platform architecture）。PSPA 涵盖了密码加速引擎、密钥管理、可信启动、可信执行环境、安全存储、固件管理、量产注入、生命周期管理、抗物理攻击及硬件漏洞免疫 10 个方面。

可信启动是指安全处理器启动过程中所有被执行的代码、引入的数据都是通过度量认证的，在启动过程中建立一条基于逐级验签认证的信任传递链。可信启动的前提是存在一个无需验证、确保可信的基础启动模块可信根。在 PSPA 规范中，可信根存储在片内不可篡改的存储介质中，由可信根对下一步启动流程引入的代码、数据进行验签。被可信根验签过的代码在执行时会对由其引入的代码和数据进行验签，以此类推，整个启动过程，各模块必须对由其引入的代码和数据进行验签以实现可信链的传递，保证整个启动过程执行的所有代码和数据都是可信的，安全的。

基于 E2000D 的工业物联数采安全终端在可信启动方面，E2000D 的启动固件由飞腾基础固件（PBF，phytium base firmware）和系统固件（SFW，system firmware）构成，E2000D 的引导固件需要通过 PBF 对 Linux 系统引导 U-Boot 进行可信封装，实现对 Linux 系统内核和文件系统的安全引导，从源头构建安全可信执行环境。

开放安全套接层（OpenSSL，open secure sockets layer）是一个开放源代码的基于 C 语言的 SSL 软件库包，应用程序可以使用这个 SSL 包来进行安全通信，避免窃听，同时确认另一端连接者的身份。

作为一个基于密码学的安全开发包，OpenSSL 提供的功能相当强大和全面，囊括了主要的密码算法、常用的密钥和证书封装管理功能以及 SSL 协议，并提供了丰富的应用程序供测试或其它目的使用。

OpenSSL 实现了 SSL 协议的 SSLv2 和 SSLv3，支持了其中绝大部分算法协议。OpenSSL 也实现了 TLSv1.0。

OpenSSL 支持丰富的对称加密、非对称加密和信息摘要算法。在对称加密方面，共支持 8 种，1 种流加密算法，7 种分组加密算法，包括 AES、DES、Blowfish、CAST、IDEA、RC2 和 RC5。支持 DH、RSA、DSA 和椭圆曲线 4 种非对称加密算法。支持 DM2、DM5、SHA、RIPEMD 五种主流的信息摘要算法，用于数字签名。OpenSSL 作为最为流行的 SSL 协议开源库，在各类加密通信及安全中被广泛应用。

E2000D 数采软件安全部分基于 OpenSSL 软件包进行开发。E2000D 数采软件由基础软件库、密钥证书、MQTT 应用软件、OPC UA 应用软件等组成。基础库主要包括 mqtt 动态库、OPC UA 动态库、openssl 动态库及 glibc 等库组成。软件配置如表 1 所示。

表 1 安全终端核心配置表

序号	系统组件	配置
1	内核	Linux Kernel 4.19
2	文件系统	BusyBox1.35
3	MQTT 库	paho.mqtt.c 1.3.12
4	OPCUA 库	Open62541 1.3
5	OpenSSL 库	OpenSSL 1.1.1u
6	编译环境	Linaro GCC 7.5

2.2　终端硬件设计

E2000D 是飞腾自主研制的国产嵌入式处理器，集成两个 FTC310 核，主频 1.5 GHz。兼容 ARM-V8 指令集，支持 64 位和 32 位指令。该处理器拥有丰富的数据接口，包括高速串行计算机扩展总线（PCIe，peripheral component interconnect express）、千兆以太网、通用串行总线（USB，universal serial bus）、安全数字输入输出（SDIO，*sec*ure digital input and output card）、串行外设接口（SPI，serial peripheral interface）、通用异步收发器（UART，universal asynchronous receiver/transmitter）等。

基于 E2000D 的工业物联数采终端核心硬件包括 2 颗粒容量为 8GB 的双倍数据率同步动态随机存取存储器（DDR，double data rate synchronous dynamic random access memory）、1 颗载板 32 GB 的内嵌式多媒体存储卡（EMMC，embedded multi media card）、2 路千兆以太网、2 路控制器局域网总线（CAN，controller area network）、1 路 RS-232、2 路 RS-485、1 路第四代移动通信（4G，the 4th generation mobile communication）。

硬件采用核心板外接扩展板的方式设计，以实现模块化复用。核心板主要由 E2000D 处理器、DDR、EMMC、四线串行外部闪存（QSPI Flash，Quad SPI flash）构成一个 E2000D 最小核心系统，CPU 的所有引脚通过接插件引出供扩展板卡使用。系统运行时，基础固件存放于 QSPI Flash 中，操作系统及文件系统存放在 EMMC 中。

扩展板用于实现数采安全终端的各类接口，为数采安全终端的数据采集与通信提供保障。以太网是扩展板的核心通信接口，采用国产裕太微 YT8521SH 芯片，支持自适应 1 000/100/10 Mbps 通信速率。YT8521SH 通过吉比特介质独立接口（RGMII，reduced gigabit media independent interface）与 E2000D 连接，实现以太网数据的可靠安全传输。

2.3　终端 MQTT 安全设计

MQTT 是目前工业物联网终端实现与云平台通信的主流协议，其具有实现简单、资源消耗小、占用带宽低等优点。但由于其轻量化的特性而在安全性能方面存在不足。文献［16］从安全认证、访问控制、数据完整性和数据机密性分析了 MQTT 协议存在的安全问题。

1）MQTT 通过明文报文传输用户名和密码进行接入验证，客户端对代理服务器并未进行安全认证，且明文用户名密码容易被截获而导致安全问题。

2）在订阅发布时，可以通过主题进行访问控制，但通配符的使用会导致部分主题不受访问限制。

3）被盗取用户名和密码后的监测客户端可以后台接入破坏数据完整性。

4）协议未给出规范的加密手段，Payload 明文传输，通信可能会被拦截、修改、重定向或者泄露，甚至会被虚假控制报文注入，安全风险高。

MQTT 作为一种应用层协议，其安全性通常可以从应用层、传输层和网络层 3 个层面来考虑。基于 E2000D 工业物联数采安全终端在传输层和应用层之间引入了 OpenSSL 库，通过 SSL 协议设计双向认证和 TLS 传输加密的 MQTT 安全策略。MQTT 安全传输的框架如图 3 所示。一条 MQTT 消息将会经过物理层、数据链路层、网络层、传输层和应用层。MQTT 的明文消息在通过网络各层都有被窃取、篡改的风险。消息的加密传输是一种有效杜绝窃取、篡改的安全手段。

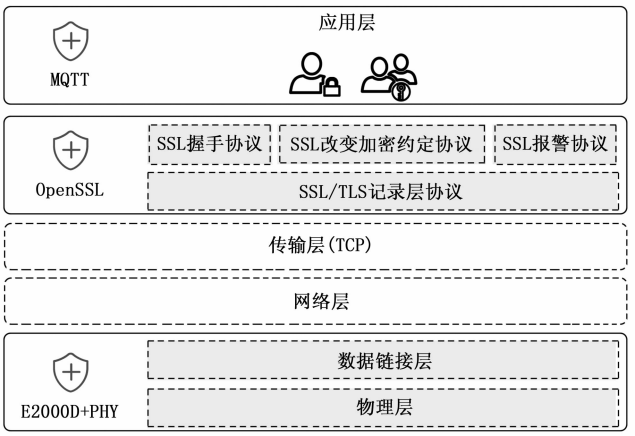

图 3　MQTT 安全传输框架

基于 E2000D 工业物联数采安全终端的 MQTT 应用程序基于 paho. mqtt. c 开源库开发。Paho. mqtt. c 是 Eclipse 编写的开源 mqtt c 库，支持 Linux、Android 和 Windows 等操作系统。Paho. mqtt. c 支持 MQTT3. 1、MQTT5. 1、LWT、Automatic Reconnect、Offline Buffering、Message Persistence、WebSocket Support、Standard MQTT Support、High Availability 等全部 MQTT 协议客户端特征。其提供了 MQTTClient 和 MQTTAsync 两套应用接口。其中 MQTTClient 接口采用同步模式，MQTTAsync 采用异步模式。

基于 E2000D 工业物联数采安全终端 MQTT 应用在 paho. mqtt. c 的基础上对物理层、数据链路层、应用层 3 层进行了改进，引入了安全策略。

物理层和数据链路层运行在国产处理器 E2000D 和国产以太网等芯片构建的可信执行环境之上。固件通过基于 PSPA 安全规范的 PBF 封装后通过网络或者 Flash 烧写器烧写到 QSPI Flash 中。E2000D 启动时，先从芯片内置的飞腾启动 ROM（PBR，phytium boot ROM）开始运行，PBR 保存在飞腾安全处理器芯片内，是无法篡改的可信根。在 PBR 启动后，导入飞腾基础固件 PBF，导入时 PBR 会对其导入的 PBF 进行验签，确保导入二级固件 PBF 的安全性。在被 PBR 验签成功后，PBF 进行处理器的基础硬件初始化，通过系统引导固件 U-Boot 的加载和验签，确保其引入代码的安全性，建立可信链。U-Boot 是可信启动的最后一级，其主要功能是进行基础外设初始化和对系统的引导与验签。从 E2000D 的一级引导到安全固件引导再到外设驱动都提供了安全监护和安全认证机制，杜绝了非法系统的运行，为

MQTT 应用程序的运行提供了安全可信的运行环境。

为了解决 MQTT 消息的明文传输带来的安全问题，在应用层和传输层之间加入安全子层，实现传输层数据经过 SSL/TLS 加密、X509 证书的认证及密钥安全协商与交换后，进行密文传输。应用层的 MQTT 通过用户名密码在 CONNECT 消息时加密进行接入访问控制，客户标识进行鉴权以实现接入安全控制。双向认证和加解密流程如图 4 所示。

基于 OpenSSL 的 MQTT 安全通信经过证书申请、双向认证和加密通信 3 个阶段。

1）证书申请，MQTT 的 Client 和 Broker 都需生成自己的私钥，并根据私钥和自身信息生成证书申请文件交由 CA 中心进行证书申请，通过证书审核后将向 Client 和 Broker 签发携带公钥和注册信息的证书。只有获得证书的 Client 和 Broker 才能进行双向认证的加密通信。

2）双向认证，整个认证过程需要经过 10 步，需要身份验证，进行证书和密钥的交换，获取对方的证书并协商加密通信所需要的加密算法的密钥。证书和密钥交换都使用密文方式进行，以保障安全性。

3）加密通信，使用协商好的加密算法对 MQTT 的接入、确认、发布等环节的数据进行对称加密。

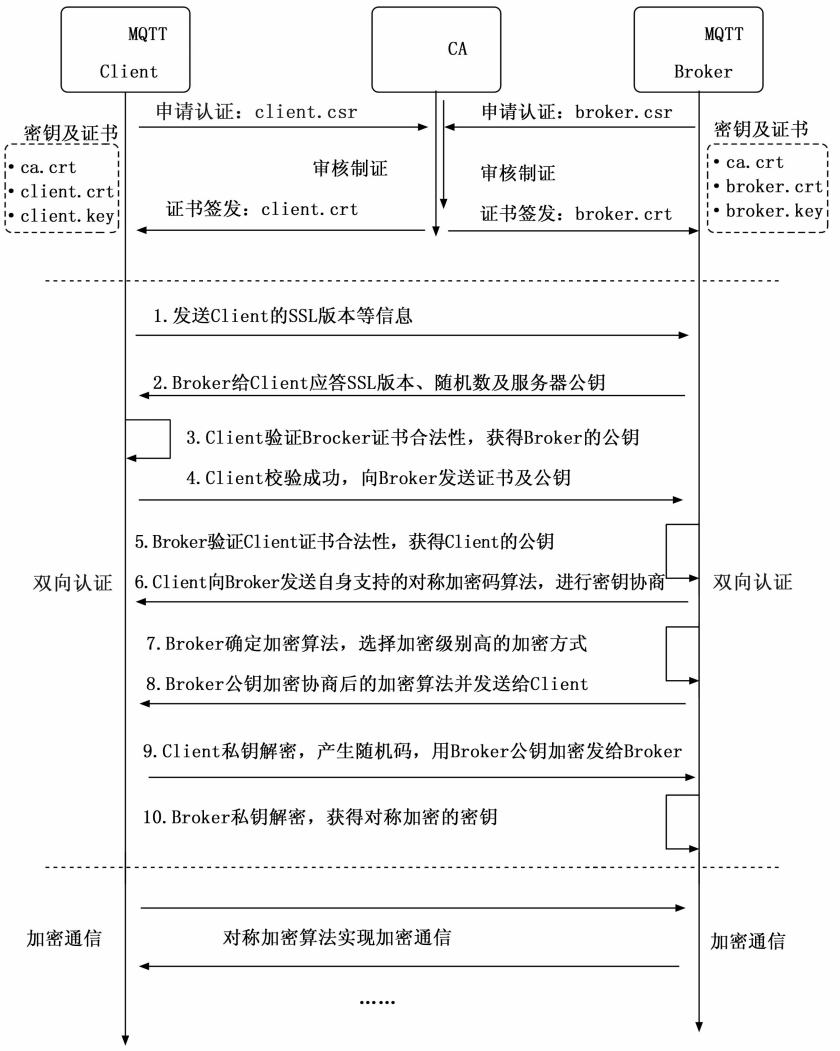

图 4 基于 OpenSSL 的 MQTT 通信流程

2.4 终端 OPC UA 安全设计

OPC UA 是在对象链接和嵌入式技术在过程控制方面应用（OPC，object linking and embedding for process control）的基础上发展起来的跨平台工业网络通信协议，被誉为工业 4.0 的先行者[17]，成为连接企业计算机与嵌入式自动化组件的桥梁，在工业自动化数据采集和工业控制中起着举足轻重的作用。

OPC UA 统一协议规范在提出之初就将安全列入协议规范中，在核心规范的第二部分[18]规定了 OPC UA 客户端和服务器之间的安全交互模型。OPC UA 的安全架构分为传输层、通信层和应用层共 3 层[19]。传输层通过套接字发送数据。OPC UA 带有错误恢复和拒绝访问机制，可以保障传输的可用性和安全性。通信层通过安全加密和数字签名保障数据的机密性和完整性，通过认证和授权进行访问控制，建立安全通道。应用层的安全机制在会话服务上实现，用于用户和产品的认证与授权。

Open62541 是一款基于 C 语言实现的 OPC UA 通信库。该库实现了 OPC UA 标准的客户端和服务器端，并支持各种操作系统和编译器。该 OPC UA 通信库功能丰富、易于移植、可扩展性好、性能优越，被广泛应用于工业自动化、智能制造、物联网等领域的数据采集，是开发 OPC UA 的一个重要选择，其具备开源免费、高度可扩展、容易移植、高性能、多线程、可嵌入性强的优点。

Open62541 支持 OPC UA 二进制协议栈以及客户端和服务器开发支持包。支持通讯栈、信息模型、订阅和代码生成等功能。

通讯栈包括 OPC UA 二进制协议栈、大信息分块、可交换网络层插件、加密通信、客户端异步服务请求等。

信息模型支持包括方法节点在内的所有节点类型；支持在运行时间添加和删除节点和引用；支持对象和变量类型的继承和实例化；单个节点访问控制。

订阅功能支持订阅或监视项目以获得数据更新通知；支持基于事件的服务器体系结构，每个受监视的资源开销都非常低。

代码生成功能支持从标准 XML 定义生成数据类型；支持从标准 XML 定义生成信息模型和节点集。

基于 OPC UA 安全模型，在 E2000D 国产化平台提供安全可信物理层和数据链路层的基础上，通过 OpenSSL 带有的密码库和 SSL 安全协议，实现对 OPC UA 通信过程中

的认证、加密、访问控制等。基于 E2000D 和 OpenSSL 的 OPC UA 安全模型扩展如图 5 所示。

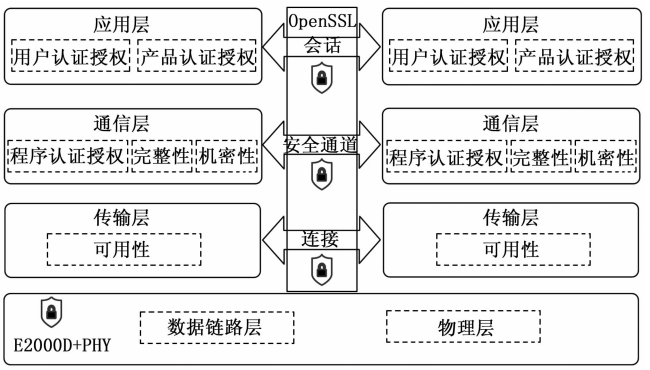

图 5　OPC UA 安全扩展模型

基于 E2000D 工业物联安全数采终端从登录方式、安全模式和安全策略共 3 方面基于 E2000 国产化平台和 OpenSSL 库，实现 OPC UA 的安全通信。

登录方式用于对服务器和客户端的访问进行控制，包括匿名登录、用户名密码登录和证书登录共 3 种方式。

安全模式决定了 OPC UA 的安全级别，支持无安全策略、签名和签名加密 3 种模式，其中签名加密安全等级最高。

安全策略决定了安全密钥的强度，包括签名算法、消息体加密和密钥包装加密共 3 类。基于 OpenSSL 在工业物联数采安全终端设计实现了以下 5 种安全策略，如表 2 所示。

表 2　安全模式与安全策略

安全策略	签名	加密
Basic128Rsa15	SHA-1	RSA
Basic256	SHA-1	RSA
Basic256Sha256	SHA-256	RSA
Aes128Sha256RsaOaep	SHA-256	RSA-OAEPAES-128
Aes256Sha256RsaPss	SHA-256	RSA-PssAES-256
None	—	—

基于 E2000D 工业物联数采安全终端南向通过 OPC UA 进行数据采集时，需要依赖于北向 MQTT 下发的数采模型。数采模型包括了 OPC UA 服务器的 IP 地址、端口号、登录方式、安全模式、安全策略、数据点位等。只有配置了采集模型的客户端才能实现数据的正常采集。数采安全终端南向 OPC UA 数采应用程序基于 open62541 协议库和 openssl 库开发，数据采集的主流程如图 6 所示。首先需要通过北向 MQTT 下发数采物模型，OPC UA 应用程序从数采模型中导入服务器接入点，加载私有证书和密钥，信任服务器证书、创建客户端句柄，并从模型中导入登录方式、安全模式和安全策略、导入采集点位和控制点位后通过 SSL 协议连接服务器。上述 9 个环节若有一个环节出现异常，连接服务器将会拒绝数采安全终端接入。在成功链接服务器后，将通过对称加密的方式实现从服务器端获取采集点位数据并解密，并将控制点位数据加密发送给服务。实现数据加密传输。

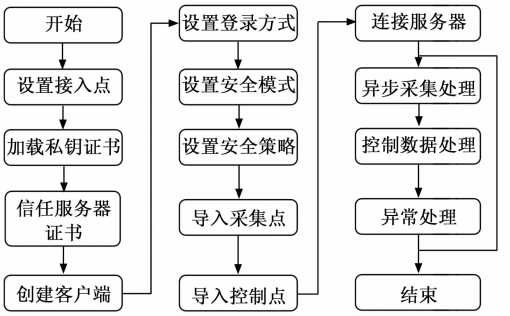

图 6　OPC UA 数据采集主体流程

3　终端测试验证

3.1　测试环境搭建

在基于 E2000D 工业物联数采安全终端的硬件上构建自主安全可信环境，基于 OpenSSL 优化并实现北向 MQTT 和南向 OPC UA 的认证与密文传输。搭建基于以太网通信的测试系统。测试系统由 2 台笔记本电脑，1 台交换机和 1 台 E2000D 工业物联数采安全终端组成，测试系统如图 7 所示。

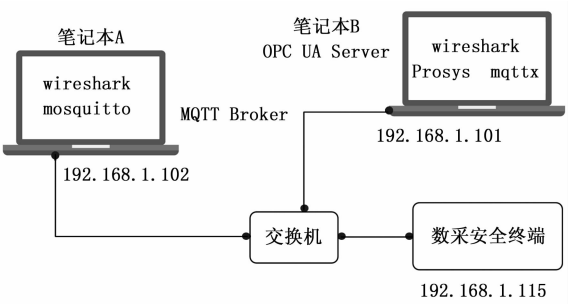

图 7　测试系统连接图

其中笔记本电脑 A 安装了 MQTT 服务器 moquitto，配置 moquitto 支持 SSL/TLS、用户名密码登录，安装 WireShark 网络抓包工具。笔记本电脑 B 安装 OPC UA 模拟服务器 ProSys Simulation Server、MQTTX 客户端工具、网络抓包工具 WireShark。E2000D 工业物联数采终端主要由 paho. mqtt. c 运行支撑库[20]、open62541 运行支撑库[21]、openssl 支撑库、MQTT 应用程序、OPCUA 应用程序、密钥和证书组成。测试系统的主要配置如表 3 所示。

表 3　测试系统配置

序号	系统组件	配置
1	MQTT 服务器	moquitto 2.0
2	OPCUA 服务器	ProSys Simulation Server 5.4.6
3	MQTT 客户端	MQTTX1.9.6
4	抓包工具	WireShark4.0.8
5	电源	DC12V

基于 E2000D 工业物联数采安全终端设计了通过 MQTT 下发南向 OPC UA 数采模型的功能，数采模型包括了 OPC UA 对应数采的设备名称、设备接入地址、设备接入端口号、登录方式、安全模式、安全策略、数据采集点位、采集点数据类型和数据采集周期等。

3.2 终端安全测试

测试时，先运行 ProSys Simulation Server 作为 OPC UA 的服务器。Prosys OPC UA Simulation Server 提供可连接到任何变量的预定义仿真信号。可以在信息模型的帮助下模拟真实设备的数据。这些信号还可以根据 OPC UA 规范提供历史数据模拟。支持多种连接类型和所有标准 OPC UA 安全模式和策略。能够测试与所有 OPC UA 应用程序的相应连接。可以启动反向连接在不打开特定端口的情况下通过防火墙。

该服务器软件支持 OPC UA 常用的登录方式、安全模式和安全策略可配置。OPC UA 服务器接以太网 3，设定 IP 地址为 192.168.1.101。

MQTT 服务器采用 moquitto 运行在笔记本电脑 B 上，mosquitto 是一款开源的 MQTT 消息代理（服务器）软件，实现了 MQTT 协议版本 3.1 和 3.1.1，提供轻量级的，支持可发布/可订阅的消息推送模式。支持配置成 SSL/TLS 安全模式。设定 moquitto 服务器的 IP 地址为 192.168.1.102，用于与基于 E2000D 工业物联数采安全终端的 MQTT 客户端进行通信。

基于 E2000D 工业物联数采安全终端的 MQTT 和 OPC UA 协议属于客户端，通过以太网联接到交换机上，实现设备互联。在基于 E2000D 工业物联数采安全终端上配置 MQTT 接入的地址、端口号、用户名和密码，采用 SSL/TLS 方式链接 moquitto 服务器。

在笔记本电脑 B 上通过 MQTTx 调试助手订阅 E2000D 工业物联数采终端的发布置主题/gateway/rtg，以/edge/model 主题向基于 E2000D 的工业物联数采终端下发数采模型，采集 3 个点位的数据。在完成配置后，基于 E2000D 工业物联数采终端可以进行正常的数据采集并实现数据上传至 MQTT 服务器中，在笔记本 B 的 MQTTx 调试助手中可以观测到相应的数据。通过 WireShark 抓包从安全认证、访问控制、数据完整性和数据机密性 4 个指标进行测试。测试结果如表 4 所示。

表 4 数采终端安全评估

协议	认证	访问控制	完整性	机密性
MQTT	√	√	√	√
OPC UA	√	√	√	√

通过 WireShark 抓包分析表明 MQTT 和 OPC UA 都可以通过 SSL 安全协议进行双向认证，通过用户名和密码进行访问控制，MQTT 还可以通过主题限制访问，OPC UA 可以通过证书进行登录控制。OPC UA 采集服务器数据通过 MQTT 上传至 moquitto，通过 MQTTx 调试助手订阅，可以接收到相应主题的数据，将数据与 OPC UA 服务器的数据进行对比验证数据是完整性的。

通过 WireShark 的流分析工具，任意抓取一包 MQTT 的数据进行机密性分析，如图 8 所示。试验表明，数据采用密文传输，无法解析数据包内容。

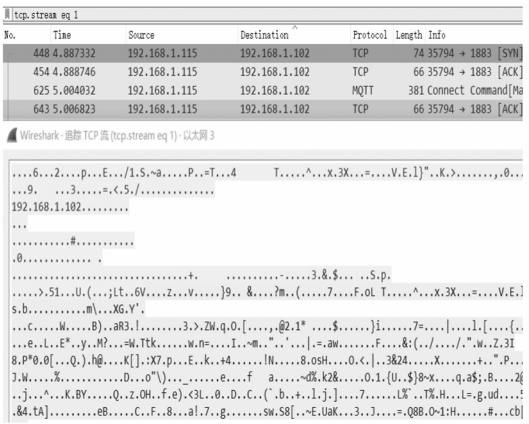

图 8 MQTT 数据机密性

同理，通过 WireShark 任意抓取 OPC UA 的数据包，可以看到数据包的消息体也是密文进行传输，无法解析到具体的数据，如图 9 所示。

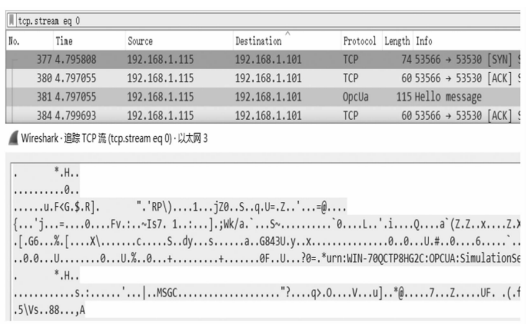

图 9 OPC UA 数据的机密性

4 结束语

基于 E2000D 工业物联数采安全终端是工业互联网安全数据采集环节中的一个重要设备。针对数采终端的安全性，就终端运行环境、北向 MQTT 协议和南向 OPC UA 协议的安全进行了深入研究，提出了一种基于国产自主可控硬件环境的工业物联数采安全终端方案，在国产硬件上，基于可信引导构建了可信运行环境，并基于 OpenSSL 安全库设计实现了支持 MQTT 和 OPC UA 安全传输的工业数采终端。通过搭建试验环境，从安全认证、访问控制、数据完整性和数据机密性共 4 个角度评估了基于 E2000D 的工业数采安全终端的安全性。测试表明，该数采终端在安全认证、访问控制、数扰完整性和数据机密性 4 个评估指标上都有比较好的表现，为工业物联网安全提供了一种可行的国产化工业数采安全终端解决方案。该工业物联数采安全终端在工业数据安全采集中有较大的应用价值。

（下转第 221 页）