物联网数据采集安全传输协议研究与设计*

周陈 陈积常 李雁星** 李建

南宁学院信息工程学院， 南宁 530200

摘 要 通过分析目前物联网数据采集系统中存在的身份假冒、数据窃密、数据篡改、数据重放、通信业务否认等安全风险，提出了防黑客主动攻击和被动攻击的安全需求，构建了基于国家商用密码技术的物联网数据采集安全模型，并利用 SM2/SM3/SM4 等国家商用密码算法、CA 认证、数字签名、签名验签、密钥管理、安全密码协议构建、mysql 数据库备份、Shell 脚本等技术，设计了物联网数据采集安全通信协议。对协议进行了安全性分析，安全分析表明：协议能实现防黑客入侵和重要数据在传输和存储过程中的机密性和完整性保护，安全性达到了求椭圆曲线离散对数的困难水平。

关键字 物联网，数据采集，商用密码，安全传输，通信协议

Research and Design of Secure Transmission Protocol for IoT Data Collection

Zhou Chen Cheng Jichang Li yanxing Li Jian

School of Information Engineering Nanning University
Nanning 530200,China;
943667593@qq.com

Abstract--By analyzing the security risks such as identity impersonation, data theft, data tampering, data replay and communication business denial existing in the current Internet of Things data acquisition system, the security requirements of preventing active and passive attacks by hackers are proposed, and a security model of Internet of Things data acquisition based on national commercial cryptography technology is constructed. And using SM2/SM3/SM4 and other national commercial password algorithms, CA authentication technology, digital signature technology, signature verification technology, key management technology, secure password protocol construction technology, mysql database backup technology, Shell script and other technologies, designed the Internet of Things data acquisition security communication protocol. The security analysis of the protocol shows that the protocol can prevent hacking and protect the confidentiality and integrity of important data during transmission and storage, and the security reaches the difficult level of calculating the discrete logarithm of elliptic curve.

Keywords--Internet Of Things; Data Acquisition; Commercial Password; Secure Transmission; Communication Protocol

1 引 言

随着 5G/6G 移动通信技术和物联网技术的快速发展，人类即将进入万物互联的时代[1]，产业数字化、数字产业化浪潮正席卷全球。然而，物联网体系结构中的安全漏洞导致了采集数据泄露，使物联网应用处于危险境地。如何应用先进的国家商用密码技术为物联网提供安全保障，成为亟待研究和解决的重大课题。

随着物联网设备的数量急剧增加，数据在设备之间的传输变得越来越频繁和复杂。同时，物联网中的设备种类繁多，不同设备之间的通信和数据传输安全面临越来越大的挑战。国内外不少学者对物联网数据采集安全传输进行了研究，如文献[2]针对水电站安全数据采集传输过程中面临的网络安全风险，提出了基于多通道的密码解决方案，但是，方案使用了国外的密码算法 RSA 和 CRC 检验技术，这些技术在一定程度上存在着安全漏洞。文献[3]分析了民航数字集群数据传输面临的网络安全威胁，为保障民航数据信息的安全使用了国外密码算法 AES 的解决方案，根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》[4]规定，也是不符合要求的。此外，还有一些学者分别从保护物联网采集数据的机密性和完整性角度提出了解决方案[5][6]，这些都是基于 DES、SHA-1、MD5 等算法进行研究数据保护的，众所周知，这些算法存在着安全漏洞。因此，如何使用国家商用密

*基金资助：本文得到南宁学院教学质量与教学改革工程项目《网络安全》核心课程（2022BKHXK09）和南宁学院一流专业培育项目（2020YLZYPY01）资助。

**通讯作者：李雁星， 877834145@qq.com 。

码技术来保护物联网数据采集系统安全是摆在我们面前的重大研究课题[7]。

本文在研究分析物联网数据采集传输系统中面临的安全风险的基础上，提出物联网数据采集安全传输需求，构建并实现一个安全的物联网数据采集传输模型。最后，通过实现模型的安全传输功能，进一步分析物联网数据采集传输协议的安全性。

2 物联网数据采集系统模型需求分析

2.1 安全风险评估

物联网数据采集传输系统是物联网基础设施的核心组成部分，负责确保从各种物联网设备中采集的数据能够安全、可靠地传输到数据中心或云端，进而为各种应用提供关键的数据支持。 因此需要对系统可能面临的安全威胁进行详细分析，分析黑客可能的攻击方式并对其加以防范，网络上常见的黑客攻击方法分为主动攻击和被动攻击两种。

●主动攻击：黑客可以截获采集终端到数据集中器之间的通信，篡改数据后，再发送到数据集中器。黑客可以伪造成合法的采集方企图混进物联网系统，向物联网数据集中器传递大量的虚假信息，从而破坏物联网的正常运行。黑客执行对物联网的攻击，事后又否认实施过任何攻击。黑客可以将截获的采集数据或命令，延迟一段时间后再发送，达到干扰和误导物联网工作的目的。

●被动攻击：黑客接入网络信道对双方传输数据进行窃听和流量分析，以掌握尽量多的有用信息。试图从密文信息恢复出明文信息和有价值的信息。因此，需要对这些物联网设备进行隐私保护、访问控制管理、数据安全保护、通信安全保护，使其具有一定的安全防护能力。

如果对以上黑客的攻击听之任之，不仅会造成严重的网络安全事故，而且会助长黑客们的嚣张气焰，使他们变本加厉并无所顾忌地展开大规模的拒绝服务攻击，导致从一点入侵到整个安全防线崩溃的多米诺骨牌效应发生。

2.2 模型安全性需求

（1）通信双方的身份鉴别。通过实施有效的身份鉴别机制[8]，物联网能够确保数据采集设备和传输系统的身份真实，仅授权设备参与数据采集和传输。随着物联网技术不断进步，需持续更新身份鉴别机制以应对新挑战，保障数据采集安全传输的可靠性。身份鉴别在物联网中至关重要，确保通信双方身份真实，满足防主动攻击需求。

（2）关键数据的机密性和完整性：机密性防止未授权的用户访问敏感数据，完整性要求数据在存储和传输中保持原状，防止篡改或损坏，确保决策和业务运行准确可靠。随着物联网环境的复杂化，保障关键数据在分布式、多节点、无保护措施的户外环境下的安全成为重要挑战。因此，需综合运用技术手段和管理措施，确保关键数据的机密性和完整性，为物联网的安全运行提供坚实保障。

（3）通信业务的不可抵赖：在执行物联网数据采集过程中，通信业务相关方，都要使用专有或唯一的事物证明自己参与了通信业务，没有任何一方能够否认自己从事的活动。

3 物联网数据采集安全传输模型设计

3.1 设计原则

（1）遵循国家信息安全法规政策

在设计物联网数据采集安全传输模型时，首先遵循国家的相关政策和法规，包括《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国关键信息基础设施保护条例》，通过设计物联网数据采集安全模型，把依法保护信息和信息系统安全的神圣职责贯穿于研究课题始终。

（2）应用国家信息安全技术标准

GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》、GM/T 0009-2012《SM2 密码算法使用规范》，GM/T 0004-2012《SM3 密码杂凑算法》和GM/T 0002-2012《SM4 分组密码算法》是开展物联网数据采集系统模型构建的根本遵循。

3.2 架构与应用部署

物联网数据采集安全模型可归结为一个应用层、数据中心应用平台支撑层、数据集中上传层和感知传感层四层模型，模型各层之间互相依赖，上下层互相提供支持。物联网数据采集安全传输系统整体设计架构和部署如图 1 所示。各个部分介绍如下图 1。

（1）数据中心包含服务器密码机（产生密钥、存储密钥、进行密码运算），负责数据采集的前置服务器（解析通信报文，通过调用服务器密码机，从而提供数据加解密、完整性认证和身份鉴别服务），应用服务器（对采集到的物联网数据进行分析和处理），数据库服务器（存储采集设备采集到的物联网数据），前置通信服务器（主要是维持公网通信信道链路的通畅）。数据中心实现物联网数据采集、网络参数设置、网络控制三类核心业务功能。

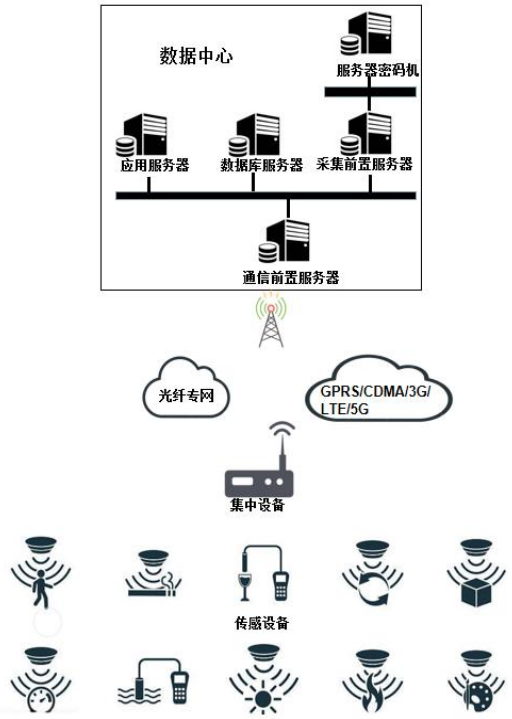

图 1 物联网数据采集安全传输模型

（2）通信信道包括 GPRS/CDMA/3G/LTE/5G 等无线和光纤网络，是物联网采集类数据上行与设置类参数、数据控制类下行的通道。

（3）数据采集集中设备和传感器设备负责收集和汇总所有的物联网原始数据，传感设备执行接收到的数据中心控制指令或设置指令；可分为数据采集集中设备子层和数据采集传感设备子层。对于超出一定数量的传感器，根据业务需求，可增加对应的集中设备，组建一个局域网，对传感器上传的感知数据信息进行汇总，由于服务器需要存储大量的物联网传感数据，其 CPU、内存容量有限，可经由集中设备将数据压缩打包后发送至数据中心。

3.3 重要设备和关键数据

（1）密码产品的部署

数据中心密码机：部署在数据中心中，通过集中前置服务器与交换机相连，用于密钥产生、存储、导入、导出与密码运算，使用了 SM2、SM3 等国家商用密码算法。设备安全芯片：部署在集中设备和传感设备内，用于数据的机密性、完整性保护与设备的身份鉴别，使用了国家商用密码算法。服务器智能密码钥匙：应用于数据中心各个通用服务器的管理员身份鉴别，使用了 SM2、SM3、SM4 等国家商用密码算法。

（2）数据中心通用服务器的部署

数据中心服务器：用于存储采集设备采集到的实时、统计以及异常事件记录等业务数据。通信前段服务器：用于维护公共网络通信信道的链路畅通；采集前端服务器：用于解析通信报文，通过调用服务器密码机来提供身份鉴别、数据加解密和完整性验证服务。应用服务器：对采集的数据进行分析、处理。

（3）数据采集网关

数据连接：它能够与各种不同类型的数据源进行连接，包括传感器、计量设备、控制系统等。为了实现这种连接，它支持多种通信协议和接口。实时数据采集：通过连接不同的数据源，数据采集网关能够实时获取来自传感器、设备、生产线等的数据。这种实时数据采集可以及时监测和获取相关数据，进而支持生产过程控制、设备状态监测等应用。数据处理和转换：网关在数据采集过程中不仅负责收集数据，还能对数据进行一系列处理操作，包括格式转换、校验以及计算等。这些处理步骤确保了数据的准确性和一致性，为后续的数据分析奠定了坚实基础。

（4）系统关键业务应用

数据采集应用：部署在数据中心的应用，主要是完成参数设置、控制指令下发、数据采集、数据管理、异常数据分析等功能。集中设备和传感设备应用：安装在采集设备和传感设备中的应用，主要是完成数据采集、安全传输等功能。

（5）数据中心关键数据

采集类业务数据：由传感设备采集的原始数据，包括实时、统计及异常事件记录等业务信息，安全需求为完整性，如果属于保密级别高的场景可按需要扩充机密性。参数类业务数据：传感设备的配置信息，可以控制数据传输格式和同步方式，根据参数的重要程度可以划分为不同级别，安全需求为同时满足机密性和完整性。控制类业务数据：控制采集设备执行动作的程序指令数据，安全需求为同时满足保密性和完整性。

4 密码应用工作流程

4.1 物联网数据采集安全传输协议流程图设计

本协议使用 SM2、SM3、数字签名技术以及数字证书实现传感设备 X、集中设备 Y、数据中心 Z 之间的双向身份认证，认证通过之后再使用 SM4 算法实现传感设备 X、集中设备 Y、数据中心 Z 之间的数据传输。协议通信符号说明如表 1 所示，物联网数据采集安全传输协议如图 2 所示。

4.2 物联网数据采集安全传输协议流程说明

（1）$ID_X||T_1||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$

传感设备 X 向集中设备 Y 发送身份、时间戳、X 对 $ID_X||T_1$ 的签名，以及 CA 签发的 X 的证书。

表 1 协议通信符号说明

符号	说明
ID_X	传感设备 X 身份
ID_Y	集中设备 Y 身份
ID_Z	数据中心 Z 身份
T	时间戳
H	杂凑值
||	拼接操作
PK_X	CA 签发的 X 的证书
PK_Y	CA 签发的 Y 的证书
PK_Z	CA 签发的 Y 的证书
SK_{CA}	证书中心 CA 的私钥
PK_{CA}	证书中心 CA 的公钥
SK_X	传感设备 X 使用 SM2 算法的私钥
SK_Y	集中设备 Y 使用 SM2 算法的私钥
SK_Z	数据中心 Z 使用 SM2 算法的私钥
PK_X	传感设备 X 使用 SM2 算法的公钥
PK_Y	集中设备 Y 使用 SM2 算法的公钥
PK_Z	数据中心 Z 使用 SM2 算法的公钥
M_1	数据
K_S	会话秘钥
E_{KS}	集中设备 Y 使用会话秘钥
Para	参数设置
Ctl	控制指令

（2）集中设备 Y 对对方进行身份鉴别的过程如下：

① 集中设备 Y 用证书中心 CA 的公钥验证 X 证书的真实性

$$CertX=D_{PKCA}[E_{SKCA}(T_2||ID_X||PK_X)]=T_2||ID_X||PK_X$$

② 用传感设备的公钥验证 X 的签名

$$H_1=D_{PKX}[E_{SKX}(H(ID_X||T_1))]=H(ID_X||T_1)$$

③ 集中设备 Y 计算哈希值 H_2

$$H_2=H(ID_X||T_1)$$

④ 判断 H_2、H_1 是否相等，如果相等则集中设备 Y 确认对方就是传感设备 X，否则无法确认对方的身份。

（3）$ID_X||ID_Y||T_3||E_{SKY}[H(ID_X||ID_Y||T_3)]||E_{SKCA}(T_4||ID_Y||PK_Y)$

集中设备 Y 向传感设备 X 发送时间戳、身份、Y 对$(ID_X||ID_Y||T_3)$的签名，以及 CA 签发的 Y 的证书。

（4）传感设备 X 对对方进行身份鉴别：

① 用证书中心 CA 的公钥验证 Y 证书的真实性

$$CertY=D_{PKCA}[E_{SKCA}(T_4||ID_Y||PK_Y)]=T_4||ID_Y||PK_Y$$

② 用集中设备的公钥验证 Y 的签名

$$H_3=D_{PKY}[E_{SKY}(H(ID_X||ID_Y||T_3))]=H(ID_X||ID_Y||T_3)$$

③ 集中设备 Y 计算哈希值 H_4

$$H_4=H(ID_X||ID_Y||T_3)$$

④ 判断 H_3、H_4 是否相等，如果相等传感设备 X 则确认对方就是集中设备 Y，否则无法确认对方的身份

（5）$E_{SKCA}(PK_X||ID_X||T_2)||E_{SKX}[H(T_5||ID_X)]||T_5||ID_X$

传感设备 X 向数据中心 Z 发送 CA 签发的传感设备 X 的证书，以及身份信息、时间戳、数字签名。

（6）数据中心 Z 对对方进行身份鉴别：

① 用证书中心 CA 的公钥验证 X 证书的真实性

$$CertY=D_{PKCA}[E_{SKCA}(T_2||ID_X||PK_X)]=T_2||ID_X||PK_X$$

② 用传感设备的公钥验证 X 的签名

$$H_5=D_{PKX}[E_{SKX}(H(ID_X||T_5))]=H(ID_X||T_5)$$

③ Z 计算哈希值

$$H_6=H(ID_X||T_5)$$

④ 判断 H_5、H_6 是否相等，如果相等数据中心 Z 则确认对方就是传感设备 X，否则无法确认对方的身份

（7）$E_{SKCA}(PK_Z||ID_Z||T_7)||T_6||ID_Z||ID_X||E_{SKZ}[H(T_6||ID_Z||ID_X)]$

数据中心 Z 向传感设备 X 发送 CA 签发的数据中心 Z 的证书，以及身份信息、时间戳、数字签名。

（8）传感设备 X 对对方进行身份鉴别：

① 用证书中心 CA 的公钥验证 Z 证书的真实性

$$CertY=D_{PKCA}[E_{SKCA}(T_7||ID_Z||PK_Z)]=T_7||ID_Z||PK_Z$$

② 用数据中心的公钥验证 Z 的签名

$$H_7=D_{PKZ}[E_{SKZ}(H(ID_Z||ID_X||T_6))]=H(ID_Z||ID_X||T_6)$$

③传感设备 X 计算哈希值 H_8

$$H_8=H(ID_Z||ID_X||T_6)$$

④ 判断 H_7、H_8 是否相等，如果相等传感设备 X 则确认对方就是数据中心 Z，否则无法确认对方的身份

（9）$E_{SKX}[H(ID_X||ID_Y||T_8||Verified\ OK)||ID_X||ID_Y||T_8||Verified\ OK$

传感设备 X 向集中设备发送身份、时间戳、确认

信息、数字签名。

（10）用传感设备 X 的公钥验证传感设备 X 的签名

① $H_9=D_{PKX}[E_{SKX}(H(ID_X||ID_Y||T_8||Verified\ OK))]=H(ID_X||ID_Y||T_8||Verified\ OK)$

② Y 计算哈希值 H_{10}

$H_{10}=H(ID_X||ID_Y||T_8||Verified\ OK)$

③ 判断 H_9 是否等于 H_{10}，如果相等则集中设备 Y 确认发送者就是传感设备 X，否则无法确认发送者的身份。

（11）$E_{SKCA}(PK_Y\ ||\ ID_Y\ ||T_4)||\ T_9||ID_Y\ ||E_{SKY}[H(T_9||ID_B)]$

① 集中设备 Y 向数据中心 Z 发送 CA 签发的集中设备 Y 的证书，以及身份信息、时间戳、数字签名。

（12）数据中心对对方身份进行鉴别：

① 用证书中心 CA 的公钥验证 Y 证书的真实性

$CertY=D_{PKCA}[E_{SKCA}(T_4||ID_Y||PK_Y)]=T_4||ID_B||PK_B$

② 用集中设备的公钥验证 Y 的签名

$H_{11}=D_{PKY}[E_{SKY}[H(T_9||ID_Y)]=H(T_9||ID_Y)$

③ Z 计算哈希值 H12

$H_{12}=H(T_9||ID_Y)$

④ 判断 H_{11} 是否等于 H_{12}，如果相等则数据中心 Z 确认发送者就是集中设备 Y，否则无法确认发送者的身份。

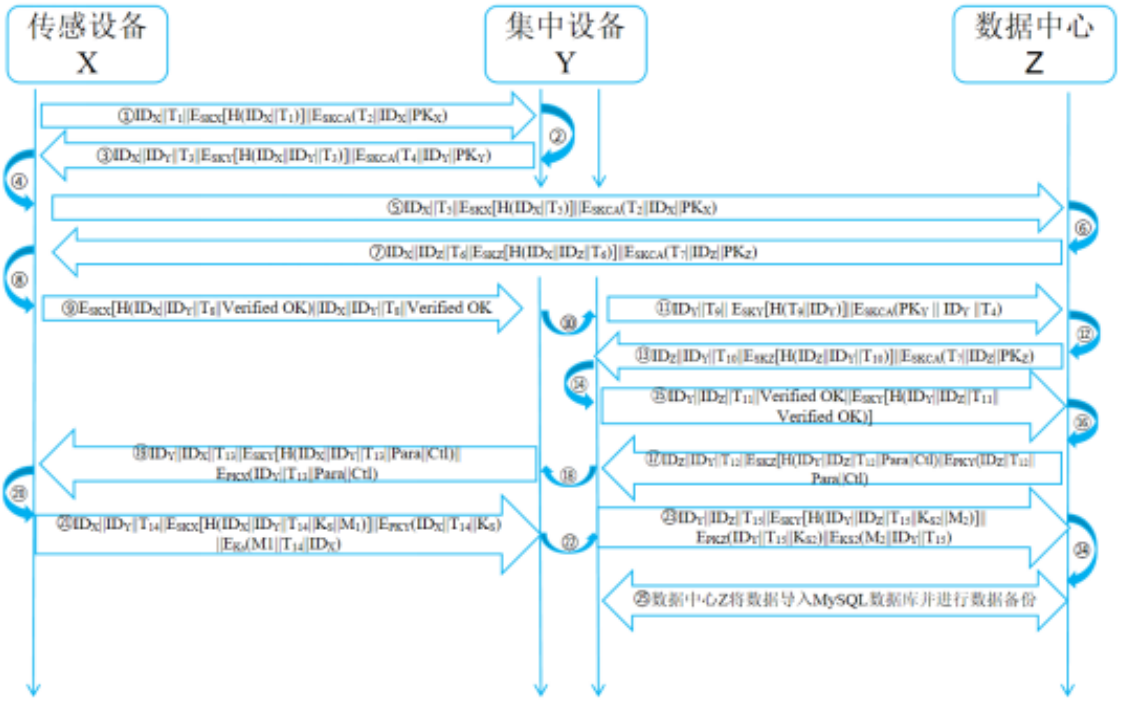

图 2　物联网数据采集安全传输协议流程

（13）$E_{SKCA}(PK_Z||ID_Z||T_7)\ ||T_{10}||\ ID_Y\ ||ID_Z\ ||E_{SKZ}[H(T_{10}||ID_Y||ID_Z)]$

数据中心 Z 向集中设备 Y 发送 CA 签发的数据中心 Z 的证书，以及身份信息、数字签名。

（14）集中设备 Y 对对方身份进行鉴别：

① 用证书中心 CA 的公钥验证 Z 证书的真实性

$CertZ=D_{SKCA}(T_7||ID_Z||PK_Z)=T_7||ID_Z||PK_Z$

② 用数据中心的公钥验证 Z 的签名

$H_{13}=D_{PKZ}[E_{SKZ}(T_{10}||ID_Y||ID_Z)]=T_{10}||ID_Y||ID_Z$

③ Y 计算哈希值 H_{14}

$H_{14}=（T_{10}||ID_Y||ID_Z）$

④ 判断 H_{13} 是否等于 H_{14}，如果相等则集中设备 Y 确认发送者是 Z，否则无法确认发送者身份。

（15）$ID_Y||ID_Z||T_{11}||Verified\ OK||E_{SKY}[H(ID_Y||ID_Z||T_{11}||Verified\ OK)$

集中设备 Y 向数据中心 Z 发送身份、时间戳、确

认信息、数字签名。

（16）用集中设备的公钥验证 Y 的签名

① $H_{15}=D_{PKY}[E_{SKY}(H(ID_Y||ID_Z||T_{11}||Verified\ OK))]=H(ID_Y||ID_Z||T_{11}||Verified\ OK)$

② Z 计算哈希值 H_{16}

$H_{16}=H(ID_Y||ID_Z||T_{11}||Verified\ OK)$

③ 判断 H_{15}、H_{16}是否相等，如果相等则数据中心 Z 确认对方就是集中设备 Y，否则无法确认对方的身份。

（17）$ID_Z||ID_Y||T_{12}||E_{SKZ}[H(ID_Y||ID_Z||T_{12}||Para||Ctl)||E_{PKY}(ID_Z||T_{12}||Para||Ctl)$

数据中心 Z 向集中设备 Y 发送 ID_Y、ID_Z、时戳 T_{12}，Z 对 $ID_Y||ID_Z||T_{12}||Para||Ctl$ 的签名值，以及用 Y 的公钥加密 $ID_Z||T_{12}||Para||Ctl$ 的值，Para、Ctl 分别为参数设置和控制命令。

（18）集中设备 Y 执行以下操作：

① 用自己的私钥进行解密

$D_{SKY}[E_{PKY}(ID_Z||T_{12}||Para||Ctl)]=ID_Z||ID_Y||Para||Ctl$

② 用数据中心 Z 的公钥解密数据中心 Z 的数字签名，得到哈希值 H17

$H_{17}=DPKZ[E_{SKZ}[H(ID_Y||ID_Z||T_{12}||Para||Ctl)]=H(ID_Y||ID_Z||T_{12}||Para||Ctl)$

③ 集中设备 Y 计算哈希值 H_{18}

$H_{18}=H(ID_Y||ID_Z||T_{12}||Para||Ctl)$

④判断 H_{17}是否等于 H_{18}，若相等则证明 Z 向 Y 发送的参数设置和控制指令 Para||Ctl 在传输过程中没有被篡改；否则 Para||Ctl 已在传输过程中被篡改，需要 Z 重传。

（19）$ID_Y||ID_X||T_{13}||E_{SKY}[H(ID_X||ID_Y||T_{13}||Para||Ctl)||E_{PKX}(ID_Y||T13||Para||Ctl)$

集中设备 Y 向传感设备 X 发送 ID_Y、ID_X、时戳 T_{13}，Z 对 $ID_Y||ID_Z||T_{12}||Para||Ctl$ 的签名值，以及用 X 的公钥加密 $ID_Y||T_{13}||Para||Ctl$ 的值，Para、Ctl 分别为参数设置和控制命令。

（20）传感设备 X 执行以下操作：

① 用自己的私钥进行解密

$D_{SKX}[E_{PKX}(ID_Y||T_{13}||Para||Ctl)]=ID_Y||T_{13}||Para||Ctl$

② 用传感设备 X 的公钥验证的签名

$H_{19}=D_{PKX}[E_{SKY}[H(ID_X||ID_Y||T_{13}||Para||Ctl)]=H(ID_X||ID_Y||T_{13}||Para||Ctl)$

③X 计算哈希值 H_{20}

$H_{20}=H(ID_X||ID_Y||T_{13}||Para||Ctl)$

④判断 H_{19}、H_{20}是否相等，若相等则证明 Y 向 X 发送的参数设置和控制指令 Para||Ctl 在传输过程中没有被篡改；否则 Para||Ctl 已在传输过程中被篡改，需要 Y 重传。

（21）$ID_X||ID_Y||T_{14}||E_{SKX}[H(ID_X||ID_Y||T_{14}||K_S)]||E_{PKY}(ID_X||T_{14}||K_S)||E_{Ks}(M_1||T_{14}||ID_X)$

传感设备 X 发送 ID_X、ID_Y、时戳 T_{14}，以及利用传感设备 X 的私钥使用 SM2 算法对 $ID_X||ID_Y||T_{14}||K_S||M_1$的哈希值进行数字签名，作用是采集设备 X 发送到集中设备 Y 的信息不可抵赖，以及用 Y 的公钥加密 $ID_X||T_{14}||K_S$的值，K_S既双方协商密钥,采集设备 X 使用 SM4 对称加密算法加密数据 M_1，时戳和身份信息。

（22）集中设备 Y 对传感设备 X 进行身份鉴别，并使用会话秘钥 KS 获取加密数据 M1：

① 用传感设备 X 的公钥验证传感设备 X 的签名

$H_{21}=D_{PKX}[E_{SKX}(H(ID_X||ID_Y||T_{14}||K_S||M_1)]=H(ID_X||ID_Y||T_{14}||K_S||M_1)$

② Y 计算哈希值 H_{22}

$H_{22}=H(ID_X||ID_Y||T_{14}||K_S||M_1)$

③ 判断 H_{21}是否等于 H_{22}，如果相等则证明加密数据 M_1以及双方协商的会话秘钥 K_S在传输的过程中没有被篡改；否则 Y 可以确认加密数据 M_1和会话秘钥 K_S在传输过程中被改变，需要重新协商。

（23）$ID_Y||ID_Z||T_{15}||E_{SKY}[H(ID_Y||ID_Z||T_{15}||K_{S2}||M_2)]||E_{PKZ}(ID_Y||T_{15}||K_{S2})||E_{KS2}(M_2||ID_Y||T_{15})$

集中设备 Y 发送 ID_Z、ID_Y、时戳 T_{15}，以及利用集中设备 Y 的私钥使用 SM2 算法对 $ID_Y||ID_Z||T_{15}||K_{S2}||M_2$的哈希值进行数字签名，作用是集中设备 Y 发送到数据中心 Z 的信息不可抵赖，以及用 Z 的公钥加密 $ID_Y||T_{15}||K_{S2}$的值，K_{S2}既双方协商密钥,集中设备 Y 使用 SM4 对称加密算法加密数据 M_2，时戳和身份信息。

（24）数据中心 Z 对集中设备 Y 进行身份鉴别，并使用会话秘钥 K_{S2}获取加密数据 M_2：

① 用数据中心 Z 的公钥验证集中设备 Y 的签名

$H_{23}=D_{SKZ}[E_{SKY}(H(ID_Y||ID_Z||T_{15}||K_{S2}||M_2))]=H(ID_Y||ID_Z||T_{15}||K_{S2}||M_2)$

② Z 计算哈希值 H_{24}

$H_{24}=H(ID_Y||ID_Z||T_{15}||K_{S2}||M_2)$

③ 判断 H_{23} 是否等于 H_{24}，如果相等则证明加密数据 M_2 以及双方协商的会话秘钥 K_{S2} 在传输的过程中没有被篡改；否则 Z 可以确认加密数据 M_2 和会话秘钥 K_{S2} 在传输过程中被改变，需要重新协商。

（25）数据中心 Z 将数据导入 MySQL 数据库并进行数据备份。

4.3 安全性分析

（1）抗身份假冒攻击

该协议通过传感设备 X、集中设备 Y 和数据中心 Z 之间的双向身份认证来抗拒身份假冒攻击。在认证过程中，传感设备 X 向集中设备 Y 发送 $ID_X||T_1||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$。集中设备 Y 通过 $D_{PKCA}[E_{SKCA}(T_2||ID_X||PK_X)]$ 和 $H(ID_X||T_1)$ 是否相等来认证传感设备 X 的身份，其中集中设备 Y 利用了传感设备 X 的公钥进行运算。同样地，传感设备 X 也能通过计算 $D_{PKCA}[E_{SKCA}(T_4||ID_Y||PK_Y)]$ 是否等于 $H(ID_X||ID_Y||T_3)$ 来认证集中设备 Y 的身份，集中设备 Y 与数据中心 Z 之间也是同理。黑客如果想要伪造签名，则需要从对方的公钥获取对应的私钥，其难度很高，几乎无法完成这一级别的破译攻击[10]。

（2）抗重放攻击

为了避免重放攻击，传感设备 X 在向集中设备 Y 发送认证请求时会包含时间戳。该时间戳是使用数字签名技术产生的数据，并能够验证消息是否实时。传感设备 X 发出的消息内容为 $ID_X||T_1||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$，消息以密文传输的。因此，如果黑客试图重放以前来自传感设备 X 的消息给集中设备 Y，则集中设备 Y 可以通过计算 $D_{PKCA}[E_{SKCA}(T_2||ID_X||PK_X)]$ 与 $H(ID_X||T_1)$ 验证时间戳的新鲜性。因此，即使攻击者发送相同的消息给集中设备 Y，集中设备 Y 验证时间戳的新鲜性，以确定是否为非法用户。

（3）抗篡改攻击

该协议抗击黑客发起的篡改攻击。当完成双方身份认证时，协议会对身份信息经行数字签名运算。例如，在传感设备 X 与集中设备 Y 之间的双向认证过程中，消息内容为 $ID_X||T_1||E_{SKX}[H(ID_X||T_1)]||E_{SKCA}(T_2||ID_X||PK_X)$，如果黑客改变了身份信息 ID_X，则 $H_1=H(ID_X||T_1)$ 将会改变，从而导致无法通过身份验证。在这种情况下，集中设备 Y 可以判断对方不是合法传感设备 X 或者传感设备 X 的身份信息被黑客篡改了。如果黑客试图同时篡改身份信息和传感设备的签名信息，则需要从传感设备的公钥获取私钥。其安全性基于椭圆曲线离散对数问题，破译难度非常高，因此使用公钥数字签名技术有效地抵抗了黑客发起的篡改攻击，并保护了信息的完整性。

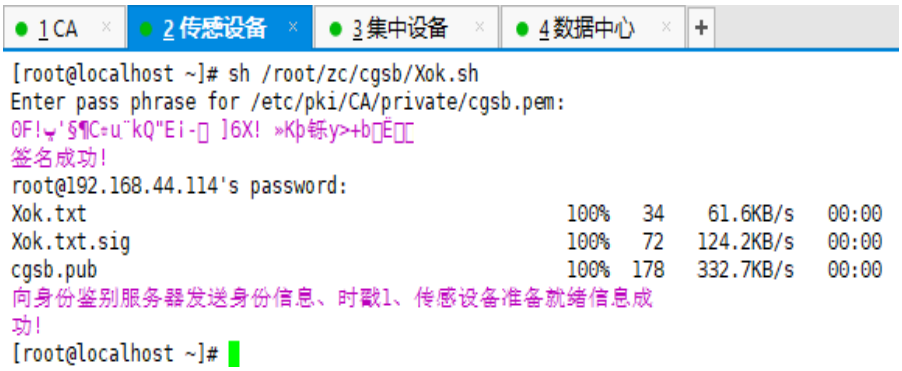

图 3 方双向身份鉴别和数据传输部分结果

（4）防非法窃听

该协议有效防止非法窃听，在数据传输时，使用 SM4 加密密钥加密数据，如传感设备 X 与集中设备 Y 的传输，SM4 算法属于对称密钥算法，其加密密钥与解密密钥相同且数据加解密速度快，适用于数据量大的场景。如果黑客使用非法手段窃取到了传输的数据，就必须使用相同的 SM4 密钥对数据经行解密，否则得到的只是一串无法解析的乱码密文。

4.4 代码运行测试

为了验证本方案设计的可行性，基于 Linux 操作系统，使用 Xshell 终端模拟软件和 GmSSL 密码工具箱，编码实现了物联网数据采集安全传输系统的功能模块和安全通信协议。三方双向身份鉴别和数据传输实现的代码运行的部分结果如图 3 所示。从代码运行的结果来看，本方案设计的物联网数据采集安全传输协议是可行有效的。

5 结束语

本文通过对物联网的工作原理和系统架构的分析，提出了国密技术在物联网数据采集安全传输领域

的应用需求，构建了基于国密技术的物联网数据采集安全传输模型。安全性分析结果表明，该模型能够实现通信双方的身份认证、关键数据传输的保密性和完整性。本文使用 Xshell 终端模拟软件和 GmSSL 密码工具箱，成功实现了协议的身份认证及数据传输功能，代码运行结果说明了物理网数据采集安全传输协议的安全性和有效性。

参 考 文 献

[1] YOU X ,WANG C ,HUANG J , et al.Towards 6G wireless communication networks:vision, enabling technologies, and new paradigm shifts[J].Science China(Information Sciences),2021,64(01):5-78.

[2] 李秀峰,李胜,梁妙元,等.基于多通道的水电站安全数据采集传输方法[J].计算机应用与软件,2023,40(05):124-128+183.

[3] 孙婷逸.民航数字集群数据传输安全研究[J].长江信息通信,2024,37(01):158-160+177.DOI:10.20153/j.issn.2096-9759.2024.01.047.

[4] 中华人民共和国国家标准.GBT 39786-2021 信息安全技术 信息系统密码应用基本要求[S].

[5] Jiazhe C,Hexin L,Beibei W.Improved chosen -plain text DPA on block cipher SM4[J].Journal of Tsinghua University(Science and Technology),2017(11):11 34-1138.

[6] Rong-Zheng C , Kun Z . One authentication scheme based on the domestic cryptographic algorithm [J]. Journal of Qiqihar University(Natural ence Edition), 2015.

[7] 李旭升.基于物联网的数据信息化采集方案研究[J].信息与电脑(理论版),2023,35(14):235-237.

[8] 郭正伟.保护物联网免受黑客攻击的基础[J].中国集成电路,2021,30(11):18-23+30.

[9] 刘红玲.数据备份与信息系统安全[J].彭城职业大学学报,1999,(04):96-98.

[10] 肖祯. 基于认证加密模式的数字证书安全性分析[J].中文信息,2021(6):2. DOI:10.12221/j.issn.1003-9082.2021.06.02.