信息采集系统安全模型设计*

刘芳 李建** 陈积常

南宁学院信息工程学院，南宁，530200

摘 要 针对目前物联网信息采集设备存在的安全问题，提出一种基于国家商用密码算法的信息采集系统安全模型，设计了一种信息采集安全通信协议，并对协议进行安全性分析。使用 gmssl 工具并运用商用密码算法、CA 认证技术、数字签名技术、签名验签技术、密钥管理技术、安全密码协议构建技术、mysql 数据库备份技术、Shell 脚本设计对安全模型进行密码应用方案设计和功能架构设计。实验测试结果，该安全模型能防入侵，实现信息采集系统重要数据在传输和存储过程中的保密性和完整性保护，安全性达到了求椭圆曲线离散对数的难度水平。

关键字 信息采集系统，CA 认证，MySQL 数据库，数字签名，商用密码算法

Design of Security Model in Information Acquisition System

Liu Fang Li Jian Chen Jichang

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

Abstract—Aiming at the current security problems for information collection equipment of Internet of Things，a security model of information acquisition system based on national commercial cryptography algorithm was proposed, the secure communication protocol of information acquisition was designed, and the security of the protocol was analyzed. By using GMSSL tool, SM2/SM3/SM4 and other national commercial cipher algorithm, CA authentication, digital signature, signature verification, key management, secure cryptographic protocol construction, MySQL database backup technology, Shell script language, the cryptography application scheme and functional architecture of the secure model was designed. The test results show that the security model can prevent intrusion and protect the confidentiality and integrity of important data in the process of transmission and storage. The security of the model is up to the difficulty level of elliptic curve discrete logarithm.

Keyword—Information acquisition system, CA certification, Mysql database; Digital signature, commercial cryptography algorithms

1 引 言

随着物联网应用向多个领域延伸，物联网安全问题日益凸显。根据 Gartner 最新发布的报告指出，近 20% 的企业机构在过去 3 年内至少观察到一次基于物联网的攻击[1]。黑客通过破解克莱斯勒汽车的自动管理系统攻入无人驾驶汽车，获取汽车自动管理系统的控制权，通过植入自己的代码，远程控制汽车的物理部件，直接威胁车乘人员生命安全；2015 年 12 月，木马网络攻击导致乌克兰局部地区持续 3 小时的电网系统停电[2]。2021 年 5 月 7 日网络黑客向美国最大燃油运输管道商科洛尼尔公司发起了网络攻击，导致该公司暂停输送业务，美国 18 个州宣布进入紧急状态。

为应对不断升级的网络安全威胁，世界各国一方面颁布了加强网络安全的法律法规[2]。另一方面开展了网络安全理论与技术的研究。我国著名密码学家王小云院士通过多年潜心研究，发现了 MD5、SHA1 等多款国外密码算法存在安全漏洞[3][4]，容易被黑客利用来发动网络攻击。由此可见，国外现有的密码算法及设备无论是主观上还是客观上都存在着安全漏洞。

国内外不少学者在物联网安全领域进行了深入研究，文献[5] 根据传感器节点的计算能力和数据存储

*基金资助：本文得到 2017 年南宁学院校级重点专业（通信工程）（2017XJZDZY11)、广西民办重点专业建设（通信工程）（2021MBZDZY01)资助.

**通讯作者：李建，教授，943667593@qq.com

容量严重受限，很多成熟的传统网络数据安全保护技术不能在物联网络中直接应用，针对无线传感器网络在隐私数据采集和传输过程中存在的安全问题，提出了基于 MD5、AES 算法的一种新型身份双向认证方案。文献[6]提出了一种可抵御已知明文攻击的物联网安全协议模型，借助 RSA、DES 密码算法解决了在信息交互过程中的身份认证、密钥分发、数据加密等问题。因此，开发具有自主知识产权的、基于国家商用密码技术的物联网安全信息采集系统已成为当务之急。

本文对目前物联网数据采集系统面临的安全威胁进行分析，提出基于国家商用密码算法设计的安全模型，设计密码应用安全协议，并对协议的安全性进行分析。在理论上的安全性得到保证的基础上，运用 PKI 技术、Linux 操作系统、SHELL 脚本编程、MySQL 数据库、数字签名技术和基于国产密码算法中 SM2、SM3、SM4 等对称分组密码算法和非对称密码算法实现安全可靠的双向身份鉴别验证、数据安全采集、存储、传输等功能。

2 信息采集系统安全模型

2.1 需求分析

随着健康、能源、交通、安防领域对物联网需求的不断扩张，物联网数据采集设备将会如雨后春笋般地涌现。物联网数据采集设备大多内部资源有限，部分暴露在没有固定的安全保护环境中，容易遭受黑客攻击，攻击的形式有主动攻击和被动攻击。

主动攻击包括非法第三方伪装成合法用户访问数据采集系统资源、截获通信双方之间的网络传输数据然后选择某个时机重放数据给这些通信方、将截获的数据按照自己的意图进行篡改后发给通信方，主动攻击会导致大量数据传输占用网络带宽，使网络通信量剧增和网速严重下降，从而导致数据采集系统瘫痪。

被动攻击主要是敌对方通过监听手段来掌握双方通信流量并进行流量分析，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。

对于信息采集系统安全模型来说，其功能需求大致如下：

（1）身份鉴别需求。信息采集系统主站的采集前置服务器与采集设备、集中设备之间进行数据交换时需要进行身份鉴别，保证通信双方身份的真实性，防止非法第三方混入数据采集系统进行破坏和捣乱，满足数据采集系统防主动攻击的需求。

（2） 关键数据存储的完整性和保密性需求。集中/采集设备分散安装在无保护措施的户外，设备内存储的一些关键数据需要采用密码技术保证其保密性和完整性，防止数据丢失或非法篡改，满足数据采集系统防被动攻击需求。

（3） 数据传输的完整性和保密性需求。信息采集系统与采集设备之间进行交换的关键数据包括采集类、参数类和控制类三类。由于上述数据交换时需经过公用网络信道，需要采用密码技术保证在传输过程中的保密性和完整性，满足数据采集系统防主动攻击和被动攻击需求。

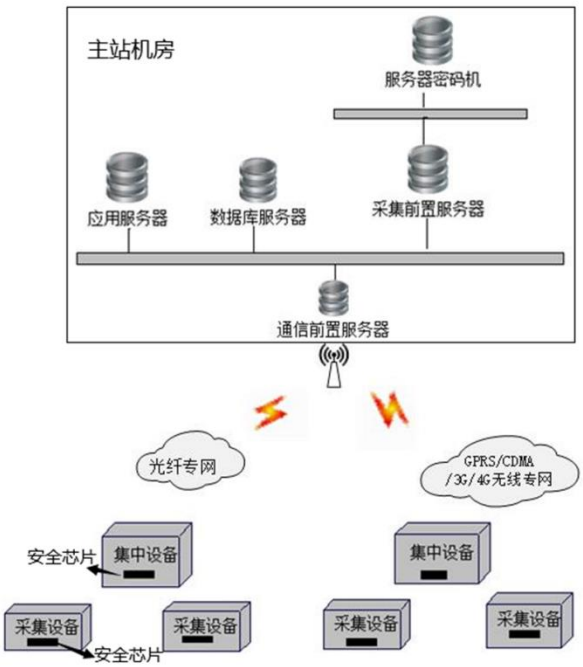

图 2-1 信息采集系统整体架构和部署图

2.2 安全模型整体设计

（1）信息采集系统整体架构与密码应用部署

信息采集系统是对分散设备信息进行自动采集、数据管理、异常数据分析以及参数和控制指令下发的信息系统，系统由主站系统、通信信道、集中设备和采集设备组成。具备点多面广、数据并发量大的特点，对实时性通信成功率要求高。为防范系统经过公网信道执行数据采集、参数和控制指令下发操作时，出现第三方非授权假冒截获、重用、篡改关键数据信息等风险，密码应用方案设计的重点在于主站和采集设备之间的身份鉴别，以及系统重要数据在传输和存储过程中的保密性和完整性保护。

信息采集系统安全模型可归结为一个层次模型，

分为主站层、通信信道层、集中/采集设备三层，模型中各层之间互相依赖，上下层互相提供支持。信息采集系统整体架构和部署图设计如图 1 所示。

① 系统主站包含服务器密码机（密钥产生、存储、密码运算），采集前置服务器（对通信报文解析，调用服务密码机提供身份鉴别、数据加解密、完整性认证），应用服务器（对采集的数据进行分析、处理），数据库服务器（存储采集设备采集的数据），通信前置服务器（维持公网通信信道的链路通畅）。主站实现数据采集、参数设置、控制三类核心业务功能。部署在主站端的应用，用于数据采集、数据管理、异常数据分析、参数设置、控制指令下发。

②通信信道包括 GPRS/CDMA/3G/4G 等无线和光纤网络，是采集类数据上行与参数设置类、控制类数据下行的通道。

③集中设备和采集设备负责收集和汇总整个系统的原始信息，采集设备执行主站下发的控制指令或参数设置指令；可分为集中设备子层和采集设备子层。对于超出一定数量的采集设备，根据业务需求，可增加集中设备，组建局域网，对采集设备上传的采集数据信息进行汇总，由于采集系统 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采集系统。安装在集中设备和采集设备中的应用，用于完成数据采集、安全传输等功能。

3 信息采集通信协议设计

3.1 信息采集通信协议

基于国家商用密码算法，以及密钥管理、数字签名等技术，本文设计的信息采集通信协议的流程图如图 1 所示。

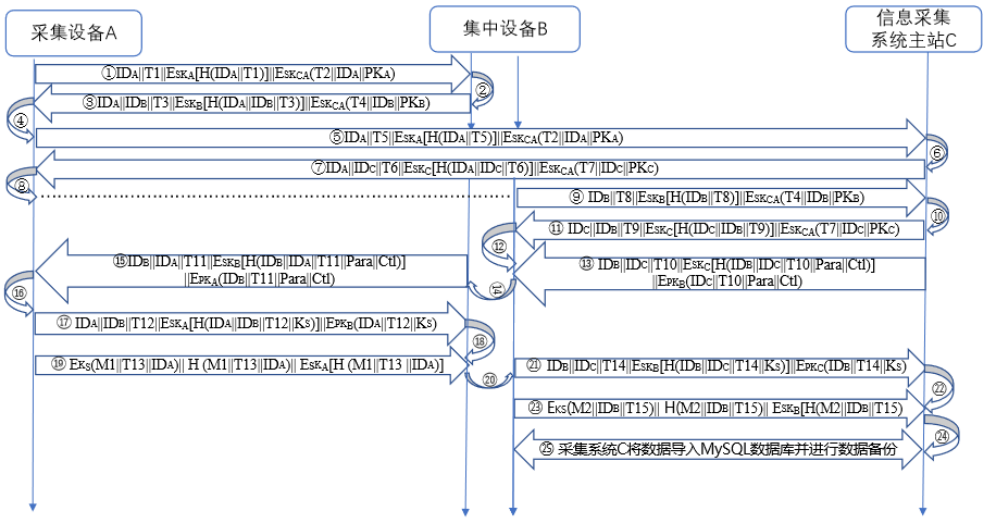

图 3-1 信息采集通信协议流程图

图 3-1 所示的信息采集通信协议流程图说明如下：

（1）采集设备 A 向集中设备 B 发送身份、时间戳、A 对 $ID_A||T1$ 的签名，以及 CA 签发的 A 的证书。

$$ID_A||T_1||E_{SKA}[H(ID_A||T_1)]||E_{SKCA}(T_2||ID_A||PK_A) \quad (1)$$

（2）集中设备对对方进行身份鉴别的过程如下：

① 集中设备用证书中心 CA 的公钥验证 A 证书的真实性，即

$$CertA=D_{PKCA}[E_{SKCA}(T_2||ID_A||PK_A)]=T_2||ID_A||PK_A \quad (2)$$

② 用采集设备的公钥验证 A 的签名，即

$$H_1=D_{PKA}[E_{SKA}(H(ID_A||T_1))]=H(ID_A||T_1) \quad (3)$$

③ B 计算哈希值 H_2

$$H_2=H(ID_A||T1) \quad (4)$$

④ 判断 H_2、H_1 是否相等，如果相等则集中设备 B 确认对方就是采集设备 A，否则无法确认对方身份。

（2）集中设备 B 向采集设备 A 发送身份、时间戳、B 对$(ID_A||ID_B||T_3)$的签名，CA 签发的 B 的证书。

$$ID_A||ID_B||T_3||E_{SKB}[H(ID_A||ID_B||T_3)]||E_{SKCA}(T_4||ID_B||PK_B \quad (5)$$

（4）采集设备对对方进行身份鉴别：

① 用证书中心 CA 的公钥验证 B 证书的真实性。

$$CertB=D_{PKCA}[E_{SKCA}(T_4||ID_B||PK_B)]=T_4||ID_B||PK_B \quad (6)$$

② 用集中设备的公钥验证 B 的签名，即

$H_3=D_{PKB}[E_{SKB}(H(ID_A||ID_B||T_2))]=H(ID_A||ID_B||T_2)$ (7)

③ B 计算哈希值 H_4，即

$H_4=H(ID_A||ID_B||T_2)$ (8)

④ 判断 H_3、H_4 是否相等，如果相等采集设备 A 则确认对方就是集中设备 B，否则无法确认对方身份。

（5）采集设备 A 向采集系统 C 发送身份、时间戳、A 对 $ID_A||T_5$ 的签名，以及 CA 签发的 A 的证书。

$ID_A||T_5||E_{SKA}[H(ID_A||T_5)]||E_{SKCA}(T_2||ID_A||PK_A)$ (9)

（6）采集系统对对方进行身份鉴别。步骤如下：

① 用证书中心 CA 的公钥验证 A 证书的真实性；

② 用采集设备的公钥验证 A 的签名；

③ C 计算哈希值；

④ 判断哈希值是否相等，如果相等采集系统 C 则确认对方就是采集设备 A，否则无法确认对方的身份。

（7）采集系统 C 向采集设备 A 发送身份、时间戳、C 对 $ID_A||ID_C||T_6$ 的签名，CA 签发的 C 的证书。

$ID_A||ID_C||T_6||E_{SKC}[H(ID_A||ID_C||T_6)]||E_{SKCA}(T_7||ID_C||PK_C)$ (10)

（8）同（2）、（4）、（6）步骤相同，即采集设备 A 对对方进行身份鉴别；鉴别通过确认对方就是采集系统 C。

（9）集中设备 B 向采集系统 C 发送身份、时间戳、B 对 $ID_B||T_8$ 的签名，以及 CA 签发的 B 的证书。

$ID_B||T_8||E_{SKB}[H(ID_B||T_8)]||E_{SKCA}(T_4||ID_B||PK_B)$ (11)

（10）同（2）、（4）、（6）步骤相同，即采集系统 C 对对方进行身份鉴别；鉴别通过确认对方就是集中设备 B。

（11）采集系统 C 向集中设备 B 发送身份、时间戳、C 对 $ID_C||ID_B||T_9$ 的签名，CA 签发的 C 的证书。

$ID_C||ID_B||T_9||E_{SKC}[H(ID_C||ID_B||T_9)]||E_{SKCA}(T_7||ID_C||PK_C)$ (12)

（12）集中设备 B 对对方进行身份鉴别；鉴别通过确认对方就是采集系统 C。身份鉴别完成之后，采集系统 C 经由集中设备向采集设备发送参数设置和控制命令。

（13）采集系统 C 向集中设备 B 发送 ID_C 、ID_B、时戳 T_{10}，A 对 $ID_B||ID_C||T_{10}||Para||Ctl$ 的签名值，以及用 B 的公钥加密 $ID_C||T_{10}||Para||Ctl$ 的值，Para、Ctl 分别为参数设置和控制命令。即

$ID_B||ID_C||T_{10}||E_{SKC}[H(ID_B||ID_C||T_{10}||Para||Ctl)]||E_{PKB}(ID_C||T_{10}||Para||Ctl)$ (13)

（14） 集中设备执行以下操作：

① 用自己的私钥进行解密，即

$D_{SKB}[E_{PKB}(ID_C||T_{10}||Para||Ctl)]=ID_C||T_{10}||Para||Ctl$ (14)

② 用 C 的公钥解密 C 的数字签名。得到哈希值 H_{14}，即

$H_{14}=D_{PKC}[E_{SKC}(H(ID_B||ID_C||T_{10}||Para||Ctl))]=H(ID_B||ID_C||T_{10}||Para||Ctl)$ (15)

③ B 计算哈希值 H_{15}，即

$H_{15}=H(ID_B||ID_C||T_{10}||Para||Ctl)$ (16)

④ 判断 H_{14} 和 H_{15} 是否相等，若相等则证明双方协商的会话密钥 Para||Ctl 在传输过程中没有被篡改；否则 B 可以确认 Para||Ctl 在传输过程中被改变，需要 C 重传。

（15）B 将 C 发送过来的参数设置和控制命令 Para||Ctl 转发给 A，即

$ID_B||ID_A||T_{11}||E_{SKB}[H(ID_B||ID_A||T_{11}||Para||Ctl)]||E_{PKA}(ID_B||T_{11}||Para||Ctl)$ (17)

（16） 采集设备执行以下操作：

① 用自己的私钥进行解密，即

$D_{SKa}[E_{PKa}(ID_B||T_{11}||Para||Ctl)]=ID_B||T_{11}||Para||Ctl$ (18)

② 用 B 的公钥解密 B 的数字签名，得到哈希值 H_{15}，即

$H_{15}=D_{PKB}[E_{SKB}(H(ID_B||ID_A||T_{11}||Para||Ctl))]=H(ID_B||ID_A||T_{11}||Para||Ctl)$ (19)

③ A 计算哈希值 H_{16}，即

$H_{16}=H(ID_B||ID_C||T_{11}||Para||Ctl)$ (20)

④ 判断 H_{15} 和 H_{16} 是否相等，若相等则证明双方协商的会话密钥 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 B 重传。

（17）采集设备 A 向集中设备 B 发送 ID_A 、ID_B、时戳 T_5，A 对 $ID_A||ID_B||T_5||K_S$ 的签名值，以及用 B 的公钥加密 $ID_A||T_5||K_S$ 的值，K_S 既双方协商密钥。即

$ID_A||ID_B||T_{12}||E_{SKA}[H(ID_A||ID_B||T_{12}||K_S)]||E_{PKB}(ID_A||T_{12}||K_S)$ (21)

（18） 集中设备执行以下操作：

① 用自己的私钥进行解密，即

$D_{SKB}[E_{PKB}(ID_A||T_{12}||K_S)]=ID_A||T_{12}||K_S$ (22)

② 用采集设备 A 的公钥解密 A 的数字签名。得到哈希值 H_{17}，即

$H_{17}=D_{PKA}[E_{SKA}(H(ID_A||ID_B||T_{12}||K_S))]=H(ID_A||ID_B||T_{12}||K_S)$ (23)

③ B 用解密得到的会话密钥 K_S 计算哈希值 H_{18}，即

$H_{18}=H(ID_A||ID_B||T_{12}||K_S)$ (24)

④ 判断 H_{17} 和 H_{18} 是否相等，若相等则证明双方协商的会话密钥 K_S 在传输过程中没有被篡改；否则 B 可确认会话密钥在传输过程中被改变，需要重新协商。采集设备 A 使用 SM4 对称加密算法加密数据 M_1，时戳和身份信息，同时使用 HMAC-SM3 算法计算数据 M_1、T_{13}、ID_A，对数据进行机密性和完整性保护；以及利用 A 的私钥使用 SM2 算法对 M_1、ID_A、T_{13} 的哈希值进行数字签名，作用是采集设备发送到集中设备的信息不可以抵赖。即

$E_{KS}(M_1||T_{13}||ID_A)||\ H\ (M_1||T_{13}||ID_A)||\ Es_{KA}[H\ (M_1||T_{13}\ ||ID_A)]$ (25)

（20） 集中设备执行以下操作：

① 利用双方协商的会话密钥 Ks，使用 SM4 对称加密算法进行解密信息，即

$D_{KS}[E_{KS}(M_1||T_{13}||ID_A)]=M_1||T_{13}||ID_A$ (26)

② 使用 HMAC-SM3 算法计算哈希值 H_{19}，即

$H_{19}=H(M_1||T_{13}||ID_A)$ (27)

③ 判断 H_{19} 和 $H(M_1||T_{13}||ID_A)$ 是否相等，如果相等集中设备可确定数据 M_1 在传输过程中没有被篡改。否则证明数据 M_1 在传输过程中被篡改需要重传。

④ 用 A 的公钥解密签名信息获取哈希值 H_{20}，计算哈希值，即

$H_{20}=H\ (M_1||T_{13}||ID_A)$ (28)

⑤ 比较 H_{20} 和 $H\ (M_1||T_{13}||ID_A)$ 是否相等，若相等集中设备 B 可确认该消息是由采集设备 A 发送的且没有被篡改，A 对发送过来的数据无法抵赖；否则无法判断该消息是由采集设备发送过来的。

（21） 集中设备 B 向信息采集系统主站发送 ID_B 、ID_C、时戳 T_{14}，B 对 $ID_B||ID_C||T_{14}||K_S$ 的签名值，以及用 C 的公钥加密 $ID_B||T_{14}||K_S$ 的值，K_S 即双方协商密钥。即

$ID_B||ID_C||T_{14}||E_{SKB}[H(ID_B||ID_C||T_{14}||K_S)]||E_{PKC}(ID_B||T_{14}||K_S)$ (29)

（22）系统主站执行以下操作：

① 用自己的私钥进行解密，即

$D_{SKC}[E_{PKC}(ID_B||T_{14}||K_S)]=ID_B||T_{14}||K_S$ (30)

② 用集中设备 B 的公钥解密 B 的数字签名。得到哈希值 H_{22}，即

$H_{22}=D_{PKB}[E_{SKB}(H(ID_B||ID_C||T_{14}||K_S))]=H(ID_B||ID_C||T_{14}||K_S)$ (31)

③ B 用解密得到的会话密钥 K_S 计算哈希值 H_{21}，即

$H_{21}=H(ID_B||ID_C||T_{14}||K_S)$ (32)

④ 判断H_{22} 和H_{21} 是否相等，若相等则证明双方协商的会话密钥K_S在传输过程中没有被篡改；否则C可以确认会话密钥在传输过程中被改变，需要重新协商。

（23）集中设备B利用会话密钥K_S使用SM4 对称加密算法加密时戳、身份信息、数据M_2（由于系统主站的CPU、内存资源有限，要将采集设备A发送的原始数据M_1 进行打包）；同时使用HMAC-SM3 算法计算数据$M_2||T_{15}||ID_B$的哈希值，对数据进行机密性和完整性保护；以及利用B的私钥使用SM2 算法对$M_2||ID_B||T_{15}$ 的哈希值进行数字签名，保证集中设备对传送到系统主站的数据不可以抵赖。即

$E_{KS}(M_2||ID_B||T_{15})||H(M_2||ID_B||T_{15})||\ E_{SKB}[H(M_2||ID_B||T_{15})$ (33)

（24） 系统主站执行以下操作：

① 利用双方协商的会话密钥 Ks，使用 SM4 对称加密算法进行解密信息，即

$D_{KS}[E_{KS}(M_2||ID_B||T_{15})]=M_2||ID_B||T_{15}$ (34)

② 使用 HMAC-SM3 算法计算哈希值 H_{23}，即

$H_{23}=H(M_2||ID_B||T_{15})$ (35)

③ 判断 H_{23} 和 $H(M_2||ID_B||T_{15})$是否相等，如果相等系统主站可确定数据 M_2 在传输过程中没有被篡改。否则证明数据 M_2 在传输过程中被非法篡改需要重新传输。

④ 用 B 的公钥解密签名信息获取哈希值 H_{24}，计算哈希值，即

$H_{25}=H(M_2||ID_B||T_{15})$ (36)

⑤ 比较 H_{24} 和 H_{25} 是否相等，若相等系统主站 C 可确认是由集中设备发送的消息没有被篡改，B 对发送过来的数据无法抵赖；否则无法判断该消息是由采集设备发送过来的。

（25）信息采集系统 C 将数据导入 MySQL 数据

库并进行数据备份。

3.2 信息采集通信协议的实施

信息采集通信协议的实现是基于 Linux 操作系统使用 Xshell 终端模拟软件和 GmSSL 密码工具箱。Xshell 可以有效地保护信息的安全性，它支持各种安全功能，如 SSH1 协议以及 RSA 公开密钥的用户认证方法，并支持加密所有流量的加密算法，Xshell 除了可以在 Windows 界面下远程控制终端之外还提供了丰富的外观配色方案；GmSSL 是一个开源的密码工具箱、标准的 OpenSSL 分支，支持 SM2/SM3/SM4/SM9/ZUC 等国家商用密码算法，提供了符合国密规范的编程接口与命令行工具 gmssl 生成 SM2 签名、SM3 摘要、HMAC-SM3 消息认证码，以及用于构建 PKI/CA、安全通信、数据加密等符合国密标准的安全应用，支持 SM4 和 ZUC 数据加解密。

（1） 三方双向身份鉴别

首先信息采集系统与集中/采集设备前往证书颁发机构(以下简称 CA 机构)为公钥做认证，获得数字证书。由于数字证书含经过权威机构认证的公钥具备安全性、唯一性，得到数字证书以后，双方通信时，只要在签名的同时，再附上数字证书就可以保证消息的真实性。具体的步骤如下：

① CA 自签根证书。首先 CA 机构 touch /etc/pki/CA/index.txt 生成证书索引数据库文件并 echo 01 > /etc/pki/CA/serial 指定第一个颁发证书的序列号，然后 CA 生成 SM2 私钥并加密私钥（cakey.pem），生成证书申请请求自签发生成根证书（cacert.pem）。

② CA 签发采集设备 A 证书。采集设备生成 SM2 公私钥对，并采用 sm2 算法加密私钥（cj.pem），然后生成包含采集设备的相关信息及公钥的证书申请文件（cj.csr），将证书申请文件发送给 CA 机构进行签发。CA 机构用根证书和私钥为采集设备签署证书（cj.crt）。待 CA 签署完毕之后将证书传送给采集设备。

③ CA 签发集中设备 B 证书。集中设备自生成 SM2 公钥私钥，加密私钥（test.pem）,然后生成包含集中设备的相关信息及公钥的证书申请文件（test.csr），将证书申请文件发送给 CA 机构进行签发。CA 机构用根证书和私钥为集中设备签署证书（test.crt）。待 CA 签署完毕之后将证书传送给集中设备。

④ CA 签发采集系统 C 证书。首先采集系统生成 SM2 公私钥对，并采用 sm2 算法加密私钥（cj.pem），然后生成包含采集系统的相关信息及公钥的证书申请文件（cj.csr），将证书申请文件发送给 CA 机构进行签发。CA 机构用根证书和私钥为采集系统签署证书（cj.crt）。待 CA 签署完毕之后将证书传送给采集系统。

⑤ A 向 B、C 发送加密身份鉴别信息。
⑥ B 向 A、C 发送加密身份鉴别信息。
⑦ C 向 A、B 发送加密身份鉴别信息。
⑧ A 对 B、C 的身份进行校验。
⑨ B 对 A、C 的身份进行校验。
⑩ C 对 A、B 进行身份校验。

（2） 参数设置与控制指令下发

采集系统 C 经由集中设备 B 向采集设备 A 下发加密参数设置、控制指令。具体实现步骤如下：

① C 向 B 传输加密参数设置和控制指令。

② B 对参数设置和控制指令进行校验。

③ B 将参数设置和控制指令转发至 A。

④ 采集设备进行校验，校验通过后，后台执行采集系统下发的参数设置和控制指令。

（3） 会话密钥协商

具体实现步骤如下：
① 采集设备向集中设备加密传输会话密钥。
② 集中设备解密获得会话密钥。
③ 集中设备与采集系统进行会话密钥加密传输。
④ 采集系统解密获得会话密钥。

（4） 数据传输及存储备份

采集设备 A 经由集中设备 B 向采集系统传输关键数据，由于采集系统 CPU、内存容量有限，B 需要将数据进行压缩打包后发送至采集系统，采集系统将数据存储至 MySQL 数据库并进行数据备份。具体实现步骤如下：

① 采集设备利用会话密钥 K1 向集中设备加密传输关键数据。

② 集中设备利用会话密钥 K1 解密获取数据。

③ 集中设备利用会话密钥 K2 将数据加密、压缩并转发至采集系统。

④ 采集系统利用会话密钥 K2 解密加密数据。

⑤ 采集系统创建 MySQL 数据库，并将数据进行存储、备份。

4 安全性分析

4.1 数字证书安全性分析

身份认证是保障网络安全的一种重要手段。用户身份鉴别利用数字证书，建立从 CA 到用户的信任链，而信任链的形成依靠公钥密码技术。

首先 CA 自签根证书。其次用户自己生成公私密钥对，私钥用于 SM2 加密，利用公钥和身份等信息生成一个证书请求发送给 CA。最后 CA 用私钥为用户签发证书，并发送给用户。

在计算哈希值时用到了国家商用密码算法 SM3，哈希值由私钥加密。且由于 CA 私钥也是使用 SM2 算法加密，它是保密的，因此证书的签名值是唯一的，不可伪造。如果黑客要伪造证书，需要对密钥进行穷搜索攻击，找到哈希函数的碰撞，复杂度达到 $O(2^n)$，对 128bit 长的哈希值来说，需要得到同一密钥产生的 264 个分组在 1Gbps 的链路上需要 25 万年。因此，伪造证书是不可能的。

4.2 三种商用密码算法安全分析

（1）国家商用密码算法 SM2 与国际标准的 ECC 算法比较其安全性体现在：一是 ECC 算法通常采用美国标准技术研究院等国际机构建议的曲线及参数，不能排除这些国际机构为了监听秘密信息的需要而故意设置漏洞的可能。而 SM2 加入了用户专有的特异曲线参数、基点、用户的公钥点信息，使得商用密码算法 SM2 的安全性明显提高。二是 ECC 算法中，用户可选择 MD5 或 SHA1 等国际通用的哈希算法，但这些算法已被证明存在严重的安全缺陷。而商用密码算法 SM2 使用 SM3 哈希算法，SM3 算法输出为 256 位，其安全性等同于 SHA-256 算法。

（2） SM3 算法的安全性主要体现在：一是抗伪原像攻击，伪原像攻击是对于给定哈希值 y，使用原根攻击方法试图找到二元组(x,IV')使得 H(x,IV')=y 的攻击方法，IV≠IV'。 通常伪原根攻击又被称为自由初值原根攻击。目前 Zoujian 等人在国际会议上提出了减小到 30 轮 SM3 密码哈希算法的伪原根攻击方法，使得 SM3 算法 30 步的原像攻击的复杂度为 2^{249}，所占内存为 2^{16}，这也是目前为止第一个对 SM3 原象攻击的结果。二是抗飞来去器攻击。目前对 SM3 算法 32 轮飞来去器攻击的复杂度差分特征概率达 $2^{14.4}$，35 轮分来去器攻击的复杂度为 $2^{117.1}$[4]。

（3） SM4 主要用于数据加密，采用 32 轮非线性迭代结构，分组长度和密钥长度都是 128 比特[7]。其安全性主要体现在使用混合整数线性规划方法(MILP)。单密钥下 27 轮的 SM4 和相关密钥下 9 轮的 SM4 都不存在概率大于 2^{-128} 的线性特征，说明 SM4 在相关密钥下抵抗线性密码分析能力较强[8]。

4.3 时戳和会话密钥作用分析

（1） 协议中的时间戳是使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。时间戳系统用来产生和管理时间戳，对签名对象进行数字签名产生时间戳，以证明原始文件在签名时间之前已经存在。可证明数据内容保持完整、未被更改。它主要是防止重放攻击。

（2） 会话密钥也称数据加密密钥或者工作密钥，是保证用户跟其它计算机或者两台计算机之间安全通信会话而随机产生的加密和解密密钥，它可由通信用户之间进行协商得到。它一般是动态地、仅在需要进行会话数据加密时产生，选择会话密钥，使其不能被攻击者预测。它是一次性用于会话中加密用的对称式密钥，所有成员使用同一把密钥来加密明文、解密密文，在此次连接结束该密钥即无效，如需重新通信则需要再重新进行一次密钥的产生及交换等步骤。

4.4 数字签名安全性分析

数字签名提供了一种安全的保障数据完整性和真实性的机制，可以检验数据从数据源到目的地的传输过程中是否被篡改以及数据的真实来源[9]。数字签名可保证用户身份的真实性，保证文件在传输过程中被篡改时，通过收文的验证能发现问题，确保数据在存储、传输和处理的过程中的安全和不可抵赖性[10]。

数字签名是先计算文件的哈希值，发送方用其私钥对哈希值进行加密；接收方用发送方的公钥进行信息解密，并对哈希值进行校验，从而确认信息的发送者身份。如果要伪造签名，就必须得到签名者的私钥，从签名者的公钥得到其私钥相当于求椭圆曲线上的离散对数，这个问题是无解的，因此，伪造签名的企图是无法实现的。

4.5 数据备份作用分析

MySQL 数据库是目前运行速度最快的 SQL 语言数据库之一[11]。利用 Linux 操作系统实现系统主站中数据库服务器的 MySQL 数据库具备自动备份功能。当采集系统管理员进行数据存储时，无意进行了修改或删除导致数据错误，甚至数据库崩溃，有效的定时备份和数据备份定时清理能很好地保护数据库数据。

4 结束语

本文分析了物联网环境下信息采集系统的安全需求，构建了信息采集系统安全模型，设计了基于国家商用密码技术的信息采集通信协议，提出了实现该安

全协议的具体思路。我们实现了物联网采集模型中设备之间的身份鉴别功能、对存储、传输数据的安全性和完整性保护，并按照安全模型、安全协议、安全分析、功能实现、使用密码算法、密码应用合规、密码应用正确、密码应用有效、抗主动攻击能力、抗被动攻击能力等维度，将本文方案与文献[5]和[6]提出的方案进行了比较。比较结果表明，本方案在密码应用合规、密码应用正确、密码应用有效、抗主动攻击能力、抗被动攻击能力等优于文献[5]和[6]提出的安全方案。

参 考 文 献

[1] 杨平,范苏洪,朱艳.基于商密 SM9 算法的物联网安全平台设计与应用[J].通信技术,2020,53(3):738-743.

[2] 颜丽.国内外物联网安全监管现状及建议[J]. 电信网技术, 2018, (1):74-76.

[3] 王小云,于红波.SM3 密码杂凑算法[J].信息安全研究,2016,2(11):983-994.

[4] 田椒陵.SM3 算法界面设计及安全性分析[J].信息安全与技术,2014,5(5):24-26+33.

[5] 白仪.面向物联网的隐私数据安全问题研究[D].天津：天津理工大学,2015.

[6] 藏传宇.一种可抵御已知明文攻击的物联网安全协议模型研究[D].昆明：云南大学,2018.

[7] 陈佳哲,李贺鑫,王蓓蓓.改进的 SM4 算法的选择明文 DPA 攻击[J].清华大学学报(自然科学版). 2017,57(11):1134-1138.

[8] 高国强.SM4 抵抗相关密钥线性密码分析的安全性[J]. 北京印刷学院学报,2020(5):154-160.

[9] 李莎, 邹勇军. 数字签名原理及实现[J]. 电脑知识与技术, 2009, 5(014):3638-3640.

[10] 陈荣征,邹昆.一种基于国产密码算法的身份认证方案[J]. 齐齐哈尔大学学报(自然科学版). 2015,31(4): 14-17,21.

[11] 马先波,冯伟.MSSQL与MySQL数据库的优劣对比及前景展望[J].科技创新导报,2009(11):19.