(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112291230 A
(43)申请公布日 2021.01.29

(21)申请号 202011154082.7

(22)申请日 2020.10.26

(71)申请人 公安部第一研究所
地址 100044 北京市海淀区首都体育馆南路1号

(72)发明人 苟智雄 徐常星 邢更力 肖瑞林 刁冯博 赵俊博 关博健

(74)专利代理机构 北京汲智翼成知识产权代理事务所(普通合伙) 11381
代理人 陈曦 任佳

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G16Y 10/75(2020.01)
G16Y 40/50(2020.01)

权利要求书2页 说明书8页 附图3页

(54)发明名称

一种用于物联网终端的数据安全认证传输方法及装置

(57)摘要

本发明公开了一种用于物联网终端的数据安全认证传输方法及装置。该方法包括:分别在物联网终端出厂预置标识密钥对,以及在边缘网关预置对应公钥矩阵;根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵,完成物联网终端和边缘网关的双向认证,并得到通信加/解密密钥;使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。有效解决传统安全手段难以物联场景需求的情况。通过轻量级的认证体制构建基于公钥密码技术实现的可应用于物联网终端上的密钥管理体系,不需要第三方的在线支持,方便实现大规模密钥产生,认证效率高,认证流程简单,并以国密算法为基础实现密码协议和密码模块,从而实现物联终端交互认证和数据加密。

CN 112291230 A

1.一种用于物联网终端的数据安全认证传输方法,其特征在于包括如下步骤:

分别在物联网终端出厂预置标识密钥对,以及在边缘网关预置对应公钥矩阵;

根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵,完成物联网终端和边缘网关的双向认证,并得到通信加/解密密钥;

使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

2.如权利要求1所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述物联网终端出厂预置标识密钥对,包括如下步骤:

向物联网终端烧录专用COS,同时在上位机软件中写入物联网终端的设备标识ID;

向所述物联网终端发送生成临时密钥对请求命令,以使得所述物联网终端响应该请求命令,生成临时密钥对,并反馈响应数据包,响应数据包中包含设备标识ID的签名值和临时公钥;

将所述响应数据包和所述设备标识ID发送到可信后台,申请下载标识密钥对,以使得所述可信后台验签成功后,生成密钥信封反馈给上位机软件;

向所述物联网终端发送导入密钥信封的命令,以使得所述物联网终端得到标识公钥,并解密出标识私钥。

3.如权利要求2所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述可信后台对所述响应数据包中的设备标识ID的签名值进行验签,若验签成功,则根据所述设备标识ID,计算出所述物联网终端的标识密钥对。

4.如权利要求3所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述可信后台通过使用所述响应数据包中的临时公钥将所述物联网终端的标识密钥对加密封装在数字信封中,得到密钥信封。

5.如权利要求2所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述物联网终端使用临时私钥解密对称密钥密文,得到对称密钥,使用对称密钥解密加密的标识私钥。

6.如权利要求1所述的用于物联网终端的数据安全认证传输方法,其特征在于:

当完成所述物联网终端到所述边缘网关的单向认证时,包括如下步骤:

接收所述物联网终端发送的使用标识私钥进行签名的认证数据包,所述认证数据包包括签名值、设备标识ID和第一随机数;

根据设备标识ID,利用内置的公钥矩阵计算对应的标识公钥,使用所述标识公钥对所述认证数据包进行验签,验签成功后生成第二随机数。

7.如权利要求6所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述物联网终端使用伪随机数生成函数或者调用其他安全模块中真随机数单元来生成所述第一随机数。

8.如权利要求1所述的用于物联网终端的数据安全认证传输方法,其特征在于:

当完成所述边缘网关到所述物联网终端的单向认证时,包括如下步骤:

接收所述边缘网关使用标识公钥加密的密文,所述密文包括第二随机数;

使用标识私钥对所接收的密文解密,解密成功,得到所述第二随机数,作为通信加/解密密钥。

9.如权利要求1所述的用于物联网终端的数据安全认证传输方法,其特征在于:

所述物联网终端与所述边缘网关中一方使用通信加密密钥通过对称加密算法SM4或SM1加密传输数据，所述物联网终端与所述边缘网关中另一方使用通信解密密钥通过所述对称加密算法SM4或SM1解密所发送的加密传输数据。

10.一种用于物联网终端的数据安全认证传输装置，其特征在于包括处理器和存储器，所述处理器读取所述存储器中的计算机程序或指令，用于执行以下操作：

分别在物联网终端出厂预置标识密钥对，以及在边缘网关预置对应公钥矩阵；

根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵，完成物联网终端和边缘网关的双向认证，并得到通信加/解密密钥；

使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

一种用于物联网终端的数据安全认证传输方法及装置

技术领域

[0001] 本发明涉及一种用于物联网终端的数据安全认证传输方法,同时也涉及相应的数据安全认证传输装置,属于网络安全技术领域。

背景技术

[0002] 随着大量物联网终端的逐步建设,泛在物联终端设备接入物联网络,对基于传统的边界安全手段建设的安全体系造成巨大威胁。在整体的物联网建设中,可对设备划分为感知层、网络层、平台层和应用层,现阶段国内外主流的安全厂商都有相对成熟完备的针对网络安全、云安全、数据安全和应用安全的整体化的解决方案,对应到网络层、平台层和应用层,所以安全能力的最大短板出现在感知层的物联网终端上。

[0003] 物联网的建设在物联网终端上面临的安全问题主要表现在三个方面能力的不足,一是身份体系缺失,二是交互数据无保护,三是设备本体安全防护不足,导致终端可能面临设备被逆向、劫持、仿冒、植毒,数据被窃取、篡改、伪造,以及终端设备供应链攻击等风险。表现在业务上即:采集数据来源、去向和内容是否可信,控制信令来源、去向和内容是否可信,终端设备是否可控。对于系统来说,表现为三个层面的安全危机:一是采集数据出现偏差,尤其是大范围、长期性偏差,导致错误的数据分析和决策依据,直接影响业务系统的运行;二是控制指令执行偏差,正确的人下发了错误的指令,或者正确的指令被错误的执行,即决策执行出错;三是终端设备本身被突破,尤其是在供应链环节,因为某几个设备的定向突破,并且被规模化复制,导致成批次的设备均被突破。

[0004] 传统的身份认证方法主要是基于公共密钥基础设施(Public Key Infrastructure,PKI)技术实现的认证系统。采用PKI技术实现身份认证具有存在如下问题:

[0005] (1)主要针对上位机与业务后台的安全认证,可以应用于网关与后台的认证,但并不适合物联网终端与网关的安全认证。

[0006] (2)由于PKI技术公钥产生不具有规模性,针对海量的多种通信协议的物联网终端统一发放证书,实际操作存在困难。

[0007] (3)证书目录需要在线运行,公钥以目录的形式存放在在线运行的目录库中,维护量大,并且无法解决物联网终端需要与网关离线认证的需求。

[0008] (4)认证可靠性依靠可信第三方证书授权中心(Certificate Authority,CA)认证链,限制了认证的灵活性。

发明内容

[0009] 本发明所要解决的首要技术问题在于提供一种用于物联网终端的数据安全认证传输方法。

[0010] 本发明所要解决的另一技术问题在于提供一种用于物联网终端的数据安全认证传输装置。

[0011] 为了实现上述目的，本发明采用下述技术方案：

[0012] 根据本发明实施例的第一方面，提供一种用于物联网终端的数据安全认证传输方法，包括如下步骤：

[0013] 分别在物联网终端出厂预置标识密钥对，以及在边缘网关预置对应公钥矩阵；

[0014] 根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵，完成物联网终端和边缘网关的双向认证，并得到通信加/解密密钥；

[0015] 使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

[0016] 其中较优地，所述物联网终端出厂预置标识密钥对，包括如下步骤：

[0017] 向物联网终端烧录专用COS，同时在上位机软件中写入物联网终端的设备标识ID；

[0018] 向所述物联网终端发送生成临时密钥对请求命令，以使得所述物联网终端响应该请求命令，生成临时密钥对，并反馈响应数据包，响应数据包中包含设备标识ID的签名值和临时公钥；

[0019] 将所述响应数据包和所述设备标识ID发送到可信后台，申请下载标识密钥对，以使得所述可信后台验签成功后，生成密钥信封反馈给上位机软件；

[0020] 向所述物联网终端发送导入密钥信封的命令，以使得所述物联网终端得到标识公钥，并解密出标识私钥。

[0021] 其中较优地，所述可信后台对所述响应数据包中的设备标识ID的签名值进行验签，若验签成功，则根据所述设备标识ID，计算出所述物联网终端的标识密钥对。

[0022] 其中较优地，所述可信后台通过使用所述响应数据包中的临时公钥将所述物联网终端的标识密钥对加密封装在数字信封中，得到密钥信封。

[0023] 其中较优地，所述物联网终端使用临时私钥解密对称密钥密文，得到对称密钥，使用对称密钥解密加密的标识私钥。

[0024] 其中较优地，当完成所述物联网终端到所述边缘网关的单向认证时，包括如下步骤：

[0025] 接收所述物联网终端发送的使用标识私钥进行签名的认证数据包，所述认证数据包包括签名值、设备标识ID和第一随机数；

[0026] 根据设备标识ID，利用内置的公钥矩阵计算对应的标识公钥，使用所述标识公钥对所述认证数据包进行验签，验签成功后生成第二随机数。

[0027] 其中较优地，所述物联网终端使用伪随机数生成函数或者调用其他安全模块中真随机数单元来生成所述第一随机数。

[0028] 其中较优地，当完成所述边缘网关到所述物联网终端的单向认证时，包括如下步骤：

[0029] 接收所述边缘网关使用标识公钥加密的密文，所述密文包括第二随机数；

[0030] 使用标识私钥对所接收的密文解密，解密成功，得到所述第二随机数，作为通信加/解密密钥。

[0031] 其中较优地，所述物联网终端与所述边缘网关中一方使用通信加密密钥通过对称加密算法SM4或SM1加密传输数据，所述物联网终端与所述边缘网关中另一方使用通信解密密钥通过所述对称加密算法SM4或SM1解密所发送的加密传输数据。

[0032] 根据本发明实施例的第二方面，提供一种用于物联网终端的数据安全认证传输装

置,包括处理器和存储器,所述处理器读取所述存储器中的计算机程序或指令,用于执行以下操作:

[0033] 分别在物联网终端出厂预置标识密钥对,以及在边缘网关预置对应公钥矩阵;

[0034] 根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵,完成物联网终端和边缘网关的双向认证,并得到通信加/解密密钥;

[0035] 使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

[0036] 本发明所提供的用于物联网终端的数据安全认证传输方法及装置适用于各种端到端的认证。在物联终端进行安全交互认证过程中,采用在物联网终端预置ECC加密密钥结构的标识密钥对,减少了对物联网终端存储资源的消耗,以及减少了传输过程中带宽的消耗;同时,本发明有效解决传统安全手段难以覆盖物联场景需求的情况。通过轻量级的认证体制构建基于公钥密码技术实现的可应用于物联网终端上的密钥管理体系,认证过程中不需要第三方在线支持,方便实现大规模密钥产生,认证效率高,认证流程简单,并以国密算法为基础实现密码协议和密码模块,从而实现物联终端交互认证和数据加密。

附图说明

[0037] 图1为本发明实施例提供的用于物联网终端的数据安全认证传输方法的流程图;

[0038] 图2为本发明实施例提供的用于物联网终端的数据安全认证传输方法中,物联网终端与边缘网关安全认证和加解密通信的示意图;

[0039] 图3为本发明实施例提供的用于物联网终端的数据安全认证传输装置的结构示意图。

具体实施方式

[0040] 下面结合附图和具体实施例对本发明的技术内容做进一步的详细说明。

[0041] 为了使本领域的技术人员更好的了解本发明,下面先对本发明实施例中出现的部分技术术语进行解释如下:

[0042] 上位机软件“预置密钥工具”:专用的定制化的生产工具,用于批量化、自动化、图形化的实现对客户端设备的密钥预置工作。该工具主体为一个.exe可执行的客户端程序。

[0043] CPK:Combined Public Key,组合公钥认证技术。

[0044] SM2:国家密码管理局于2012年公开发布成为国家密码行业标准的非对称密码算法。

[0045] SM4:国家密码管理局于2012年公开发布成为国家密码行业标准的对称密码算法。

[0046] 为了实现物联网终端与边缘网关的交互认证和加密通信,如图1和2所示,本发明实施例提供了一种用于物联网终端的数据安全认证传输方法,包括如下步骤:

[0047] 步骤S1、分别在物联网终端出厂预置标识密钥对,以及在边缘网关预置对应公钥矩阵。

[0048] 每个物联网终端在出厂时候都有对应的设备标识ID。设备标识ID一般采用如通过设备型号、规格、批次、加工厂代码、序列号、流水号等多种信息组合设计的固定长度和结构的字符序列。根据该设备标识ID,使用上位机软件“预置密钥工具”给物联网终端预置标识密钥对,这里预置成功的标识密钥对是最终归属物联网终端的设备密钥对,在后续的物联

网终端与边缘网关的双向认证和通信加密中用于设备认证、协商密钥,具体用于签名验签和传输数据的加密和解密。

[0049] 以上位机软件“预置密钥工具”为执行主体,实现在物联网终端出厂预置标识密钥对,包括如下步骤:

[0050] 步骤S11、向物联网终端烧录专用COS,同时在上位机软件“预置密钥工具”中写入物联网终端的设备标识ID。

[0051] 物联网终端内部通过串口实现数据写入和读取,“预置密钥工具”运行在上位机上,一般使用USB转串口的转换线将物联网终端和该上位机连接在一起,

[0052] 通过上位机软件“预置密钥工具”向物联网终端内的安全芯片或者其他形式的密码模块烧录专用COS(Chip Operating System,片内操作系统),用于响应上位机软件“预置密钥工具”发送的各项命令,以执行对应的操作。同时,在上位机软件“预置密钥工具”中写入物联网终端的设备标识ID。

[0053] 步骤S12、向物联网终端发送生成临时密钥对请求命令,以使得物联网终端响应该请求命令,生成临时密钥对,并反馈响应数据包,响应数据包中包含设备标识ID的签名值和临时公钥。

[0054] 当上位机软件“预置密钥工具”向物联网终端发送生成临时密钥对请求命令时,物联网终端通过专用COS接收并响应该生成临时密钥对请求命令,通过物联网终端内的安全芯片或者其他形式的密码模块生成一对临时密钥对,该临时密钥对包括临时公钥和临时私钥。同时,物联网终端将其设备标识ID进行签名,并将设备标识ID的签名值和临时公钥打包作为响应数据包反馈给上位机软件“预置密钥工具”。

[0055] 步骤S13、将响应数据包和设备标识ID发送到可信后台,申请下载标识密钥对,以使得可信后台验签成功后,生成密钥信封反馈给上位机软件“预置密钥工具”。

[0056] 上位机软件“预置密钥工具”接收到物联网终端发送的响应数据包后,将该响应数据包和物联网终端的设备标识ID发送到可信后台,并向可信后台申请下载标识密钥对。可信后台对上位机软件“预置密钥工具”发送的响应数据包中的设备标识ID的签名值进行验签,若验签成功,则根据物联网终端的设备标识ID,计算出物联网终端的标识密钥对,该标识密钥对包括标识私钥和标识公钥;可信后台通过使用响应数据包中的临时公钥将标识密钥对加密封装在数字信封中,即密钥信封,并将该密钥信封反馈给上位机软件“预置密钥工具”。可信后台为提供密钥服务及管理服务的平台。

[0057] 其中,密钥信封中的数据结构采用ECC(Elliptic Curves Cryptography,椭圆曲线密码编码学)加密密钥对保护结构(参见标准:GM/T0016-2012)。具体表示如下:

```
typedef struct SKF_ENVELOPEDKEYBLOB{
  ULONG Version;                //当前版本为 1
  ULONG ulSymmAlgID;            //对称算法标识，限定 ECB 模
式
[0058]  ULONG ulBits;             //加密密钥对的密钥位长度
  BYTE cbEncryptedPriKey[64];   //加密密钥对私钥的密文
  ECCPUBLICKEYBLOB PubKey;      //加密密钥对的公钥
 ECCCIPHERBLOB ECCCipherBlob;   //用临时公钥加密的对称密
钥密文
[0059] }ENVELOPEDKEYBLOB,*PENVELOPEDKEYBLOB;
```

[0060] 步骤S14、向物联网终端发送导入密钥信封的命令，以使得物联网终端得到标识公钥，并解密出标识私钥。

[0061] 物联网终端接收到上位机软件“预置密钥工具”发送的导入密钥信封的命令，使用临时私钥解密对称密钥密文，得到对称密钥，使用对称密钥解密加密的标识私钥，标识公钥直接在密钥信封中。因此，实现了在物联网终端出厂预置标识密钥对，该标识密钥对被存储在物联网终端的FLASH芯片中。

[0062] 其中，标识公钥的数据结构采用ECC加密公钥结构，(参见标准:GM/T0016-2012)。具体表示如下：

```
typedef struct Struct_ECCPUBLICKEYBLOB{
  ULONG      BitLen;
  BYTE       XCoordinate[ECC_MAX_XCOORDINATE_BITS_LEN/8];
[0063]  BYTE       YCoordinate[ECC_MAX_YCOORDINATE_BITS_LEN/8];
}ECCPUBLICKEYBLOB,*PECCPUBLICKEYBLOB;
```

ECC_MAX_XCOORDINATE_LEN 为 ECC 算法 X 坐标的最大长度；

ECC_MAX_YCOORDINATE_LEN 为 ECC 算法 Y 坐标的最大长度。

[0064] 标识私钥的数据结构采用ECC加密私钥结构，(参见标准:GM/T0016-2012)。具体表示如下：

```
typedef struct Struct_ECCPRIVATEKEYBLOB{
  ULONG       BitLen;
[0065]  BYTE       PrivateKey[ECC_MAX_MODULUS_BITS_LEN/8];
}ECCPRIVATEKEYBLOB,*PECCPRIVATEKEYBLOB;
```

ECC_MAX_MODULUS_BITS_LEN 为 ECC 算法模数的最大长度。

[0066] 采用ECC加密公私钥结构的好处是，ECC算法和RSA算法，在同等算法安全强度的情况下，ECC的密钥长度远小于RSA的密钥长度，而密钥长度的减少，直接带来的是计算效率的

提升,资源消耗的降低,同时在相同的密钥强度下,ECC的密钥生产的速度、加密、签名、解密的速度都要优于RSA算法。

[0067] 在边缘网关预置对应公钥矩阵时,可以把公钥矩阵设置为一个自定义的vdk格式的文件,作为文件安全的放置在网关系统中,公钥矩阵的文件名一般为pub.vdk。还可以在网关系统中烧录计算公钥矩阵的程序,以计算对应物联网终端的公钥矩阵。

[0068] 利用CPK密钥矩阵构建原理构建公钥矩阵,公钥矩阵不固定,不同的产品不同的批次不同的使用场景,根据需要可使用不同的参数生成不同的公钥矩阵,具体使用时固定一个就可以。

[0069] 利用CPK密钥矩阵构建原理构建公钥矩阵的过程如下:

[0070] 在CPK密钥体制中,给定一组椭圆曲线的参数T=(a,b,G,n,p),可建立公私钥矩阵。在这组参数下,任意选出m个元素:

[0071] X1=i1*G=(X1,y1)

[0072] X2=i2*G=(X1,y1)

[0073] ……

[0074] Xm=im*G=(Xm,ym)

[0075] (X1,i1),(X2,i2),……(Xm,im)是m个公私钥对。其中前者可以作为公钥,后者作为私钥使用。而椭圆曲线参数G就是这组公私钥的关键,在CPK的使用中,基点G需要特别保存,不可以泄露。

[0076] 步骤S2、根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵,完成物联网终端和边缘网关的双向认证,并得到通信加/解密密钥。

[0077] 当完成物联网终端到边缘网关的单向认证时,以边缘网关为执行主体,包括如下步骤:

[0078] 步骤S21、接收物联网终端发送的使用标识私钥进行签名的认证数据包,该认证数据包包括签名值、设备标识ID和第一随机数。

[0079] 物联网终端可以使用伪随机数生成函数或者调用其他安全模块中真随机数单元来生成第一随机数SK1,然后使用预置的标识私钥将设备标识ID和第一随机数SK1作为原文进行签名,将“签名值、设备标识ID和第一随机数”组成认证数据包。将物联网终端作为客户端,通过网线连接局域网中边缘网关服务器,连接成功后,发起双向认证请求,将上述认证数据包通过TCP/IP协议发送给边缘网关服务器。

[0080] 步骤S22、根据设备标识ID,利用内置的公钥矩阵计算对应的标识公钥,使用该标识公钥对认证数据包进行验签,验签成功后生成第二随机数。

[0081] 利用CPK密钥生成原理,对设备标识ID做相应运算,然后映射到边缘网关内置的公钥矩阵上,生成标识公钥。使用该标识公钥对物联网终端发送的认证数据包中的签名值、设备标识ID和第一随机数SK1进行验签,验签成功后生成第二随机数SK2。

[0082] 当完成边缘网关到物联网终端的单向认证时,以物联网终端为执行主体,包括如下步骤:

[0083] 步骤S23、接收边缘网关使用标识公钥加密的密文,该密文包括第二随机数。

[0084] 边缘网关使用标识公钥对步骤S22生成的第二随机数SK2进行加密,并将密文发送给对应的物联网终端。

[0085] 步骤S24、使用标识私钥对所接收的密文解密，解密成功，得到第二随机数SK2，作为通信加/解密密钥。

[0086] 物联网终端将接收到的边缘网关发送的密文进行解密，解密成功则完成边缘网关到物联网终端的单向认证。

[0087] 步骤S3、使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

[0088] 物联网终端与边缘网关之间传输数据的加解密过程中，物联网终端与边缘网关中某一方接收到另一方使用通信加密密钥加密的传输数据，则使用通信解密密钥进行解密，解密完成后，根据业务逻辑，完整响应操作。

[0089] 其中，物联网终端与边缘网关中一方使用通信加密密钥通过对称加密算法SM4或SM1加密传输数据；物联网终端与边缘网关中另一方使用通信解密密钥通过对称加密算法SM4或SM1解密加密传输数据。

[0090] 以物联网终端采用电力系统中配电终端，边缘网关采用位于配电房的远程监控控制网关为例，配电终端是配电开关监控终端的简称。配电开关监控终端(简称FTU)具有遥控、遥测、遥信，故障检测功能，并与配电自动化主站通信，提供配电系统运行情况和各种参数即监测控制所需信息，包括开关状态、电能参数、相间故障、接地故障以及故障时的参数，并执行配电主站下发的命令，对配电设备进行调节和控制，实现故障定位、故障隔离和非故障区域快速恢复供电等功能。

[0091] 远程监控控制网关一般包括配电房设备状态监测、配电房环境监测、配电房安防监控、配电房设备联动控制等，将相关信息上报上级单位和接收上级下发命令等。这个边缘网关一般可以是ARM高端CPU,强大边缘计算能力,Linux系统，接口丰富，方便配电房各仪表、传感器、视频等广泛接入，配备丰富的行业应用接口，包LAN口、WAN口、RS232、RS485、串口等丰富的采集控制端口，方便配电房各种仪表、传感器、摄像头等设备接入。

[0092] 配电终端通过网线与配电房监控网关连接。配电房监控网关与配电终端连接模型为客户端/服务器(C/S)模型。

[0093] 若配电终端检测到接地故障，需要将此状态通过远程监控控制网关发送给上级单位的业务平台，加密发送过程具体如下：

[0094] 配电终端将故障信息使用通信加密密钥SK2通过对称加密算法SM4或SM1加密后，将加密信息以一定的命令格式，通过网络先连接边缘网关服务器，然后发送加密信息，边缘网关服务器收到加密信息后，同样使用通信解密密钥SK2通过对称加密算法SM4或SM1解密，解密完成后，根据业务逻辑，完整响应操作。即将配电终端检测到接地故障发送给上级单位的业务平台做进一步处理。

[0095] 此外，如图3所示，本发明实施例还提供一种用于物联网终端的数据安全认证传输装置，包括处理器32和存储器31，还可以根据实际需要进一步包括通信组件、传感器组件、电源组件、多媒体组件及输入/输出接口。其中，存储器、通信组件、传感器组件、电源组件、多媒体组件及输入/输出接口均与该处理器32连接。前已述及，存储器31可以是静态随机存取存储器(SRAM)、电可擦除可编程只读存储器(EEPROM)、可擦除可编程只读存储器(EPROM)、可编程只读存储器(PROM)、只读存储器(ROM)、磁存储器、快闪存储器等；处理器32可以是中央处理器(CPU)、图形处理器(GPU)、现场可编程逻辑门阵列(FPGA)、专用集成电路

(ASIC)、数字信号处理(DSP)芯片等。其它通信组件、传感器组件、电源组件、多媒体组件等均可以采用现有智能手机中的通用部件实现,在此就不具体说明了。

[0096] 另外,本发明实施例提供的用于物联网终端的数据安全认证传输装置,包括处理器32和存储器31,处理器32读取所述存储器31中的计算机程序或指令,用于执行以下操作:

[0097] 分别在物联网终端出厂预置标识密钥对,以及在边缘网关预置对应公钥矩阵。

[0098] 根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵,完成物联网终端和边缘网关的双向认证,并得到通信加/解密密钥。

[0099] 使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密。

[0100] 本发明所提供的用于物联网终端的数据安全认证传输方法及装置适用于各种端到端的认证。在物联终端进行安全交互认证过程中,采用在物联网终端预置ECC加密密钥结构的标识密钥对,减少了对物联网终端存储资源的消耗,以及减少了传输过程中带宽的消耗;同时,本发明有效解决传统安全手段难以覆盖物联场景需求的情况。通过轻量级的认证体制构建基于公钥密码技术实现的可应用于物联网终端上的密钥管理体系,认证过程中不需要第三方在线支持,方便实现大规模密钥产生,认证效率高,认证流程简单,并以国密算法为基础实现密码协议和密码模块,从而实现物联终端交互认证和数据加密。

[0101] 以上对本发明所提供的用于物联网终端的数据安全认证传输方法及装置进行了详细的说明。对本领域的一般技术人员而言,在不背离本发明实质内容的前提下对它所做的任何显而易见的改动,都将属于本发明专利权的保护范围。

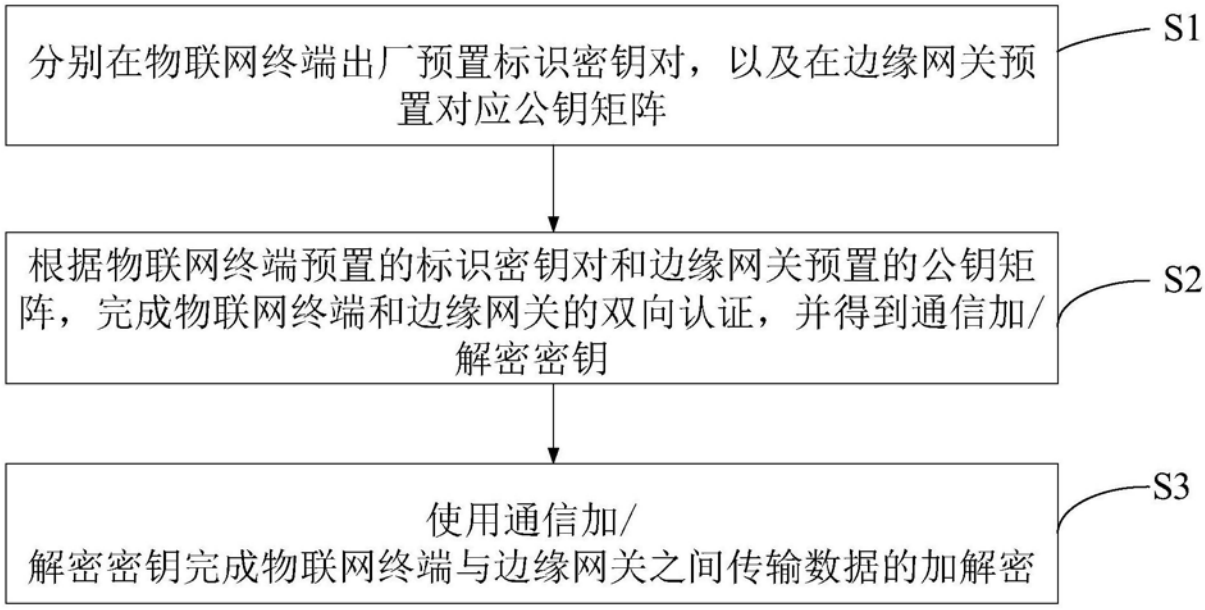
分别在物联网终端出厂预置标识密钥对，以及在边缘网关预置对应公钥矩阵
S1
根据物联网终端预置的标识密钥对和边缘网关预置的公钥矩阵，完成物联网终端和边缘网关的双向认证，并得到通信加/解密密钥
S2
使用通信加/解密密钥完成物联网终端与边缘网关之间传输数据的加解密
S3

图1

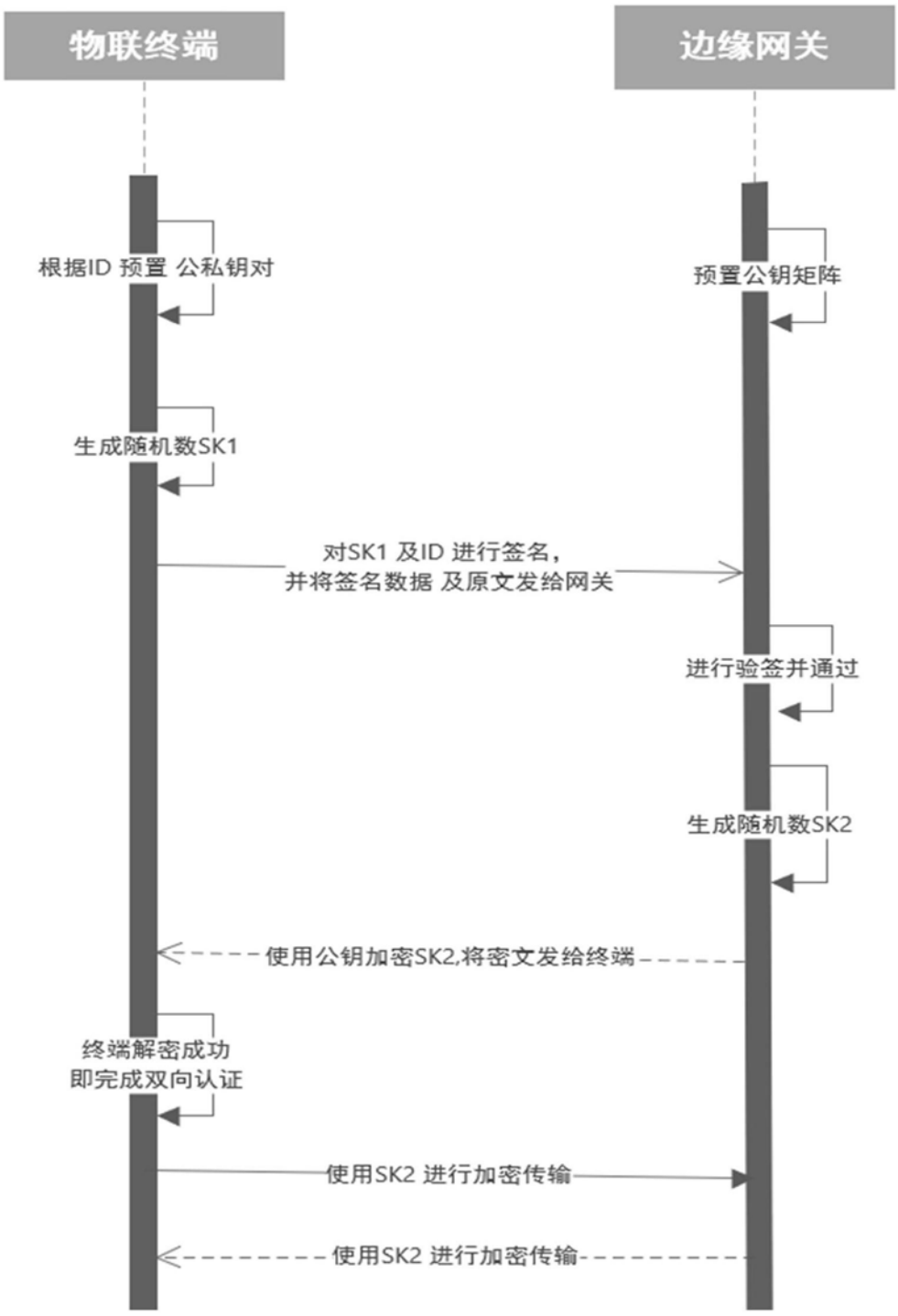
物联终端
边缘网关
根据ID 预置 公私钥对
预置公钥矩阵
生成随机数SK1
对SK1 及ID 进行签名，
并将签名数据 及原文发给网关
进行验签并通过
生成随机数SK2
使用公钥加密SK2,将密文发给终端
终端解密成功
即完成双向认证
使用SK2 进行加密传输
使用SK2 进行加密传输

图2

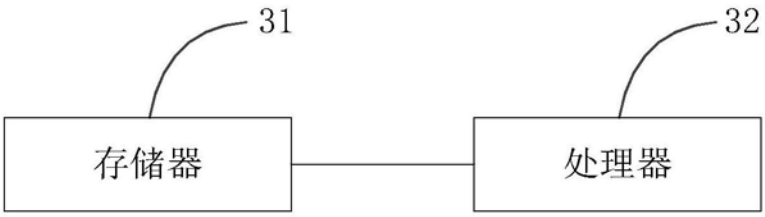

图3