(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 109995766 A
(43)申请公布日 2019.07.09

(21)申请号 201910182709.0

(22)申请日 2019.03.12

(71)申请人 浙江远望信息股份有限公司
地址 310000 浙江省杭州市滨江区丹枫路788号海越大厦15层

(72)发明人 傅如毅 安革生 邵森龙

(74)专利代理机构 杭州中利知识产权代理事务所(普通合伙) 33301
代理人 韩洪

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

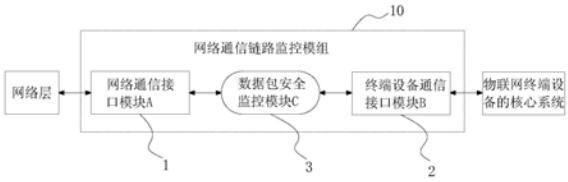
权利要求书2页 说明书4页 附图2页

(54)发明名称

基于通信链路监控对物联网设备进行网络安全防护的方法

(57)摘要

本发明提出了一种基于通信链路监控对物联网设备进行网络安全防护的方法,该方法基于一个网络通信链路监控模组,所述网络通信链路监控模组串联在物联网终端设备的网络通信链路上,功能和控制均独立于物联网设备自身的软硬件系统,所述网络通信链路监控模组被串联在物联网终端设备与网络层通信的数据链路上,物联网终端设备与网络层的所有通信均需要通过网络通信链路监控模组,数据包安全监控模块C根据内置的规则对经过的数据包进行合法性判断和处理,合法的数据包可透明传输,不合法的数据包被阻截。本发明将信任锚建立在物联网终端设备的网络通信链路上,该安全防护机制独立于物联网应用,不受物联网应用控制,通用性强,安全机制独特。



CN 109995766 A

1.基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:该方法基于一个网络通信链路监控模组(10),所述网络通信链路监控模组(10)串联在物联网终端设备的网络通信链路上,功能和控制均独立于物联网设备自身的软硬件系统,所述网络通信链路监控模组(10)包括网络通信接口模块A(1)、终端设备通信接口模块B(2)和数据包安全监控模块C(3),所述数据包安全监控模块C(3)负责对数据包进行合法性判断和处理,所述数据包安全监控模块C(3)通过网络通信接口模块A(1)与网络层通信连接,所述数据包安全监控模块C(3)通过终端设备通信接口模块B(2)与物联网终端设备的核心系统通信连接,该网络安全防护的方法通过以下方式实现:

所述网络通信链路监控模组(10)被串联在物联网终端设备与网络层通信的数据链路上,物联网终端设备与网络层的所有通信均需要通过网络通信链路监控模组(10)才能实现,所述数据包安全监控模块C(3)根据内置的规则对经过的数据包进行合法性判断和处理,合法的数据包可透明传输,不合法的数据包被阻截,从而基于通信链路监控对物联网终端设备实现网络通信安全防护功能。

2.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)的数据包安全监控模块C(3)可对经过的数据包进行解析,实施网络通信安全控制策略,所述网络通信安全控制策略包括防火墙、防病毒、入侵检测、身份认证和数据签名、数据包加解密、网络安全态势监测,根据应用场景、所防护物联网终端设备应用特性和安全要求的不同,数据包安全监控模块C(3)的安全控制策略采取上述安全技术中的一种或数种的组合。

3.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)的数据包安全监控模块C(3)可对异常通信数据包进行特征聚类、统计、缓存并通过网络上报至远程安全管理平台(4),为管理者提供海量的态势采集数据。

4.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)的数据包安全监控模块C(3)还包括管理子模块(31),所述管理子模块(31)与数据包安全监控模块C(3)通信连接,所述管理子模块(31)具备对数据包处理模块中的处理规则进行设置管理的功能,所述管理子模块(31)通过网络通信接口模块A(1)与远程安全管理平台(4)通信连接。

5.如权利要求1或4所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)还包含配置拔位开关模块(32),所述配置拔位开关模块(32)与数据包安全监控模块C(3)通信连接并控制数据包安全监控模块C(3)的设置模式,当配置拔位开关模块(32)的开关位于不同开关位时,安全监控模块C(3)的设置模式分别为不允许设置、仅允许本地设置和允许远程设置三种模式。

6.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)还包含本地配置接口模块(33),所述本地配置接口模块(33)与安全监控模块C(3)通信连接,可对数据包过滤规则、不合规数据包处理和上报规则进行本地设置,所述本地配置接口模块包括但不限于UART接口、SPI接口、IIC接口或SDIO接口。

7.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其

特征在于:所述网络通信链路监控模组(10)的网络通信接口模块A(1)、终端设备通信接口模块B(2)的接口形式包括多种标准有线通信接口,以适用于不同的物联网终端设备有线接入方式。

8.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)用于无线组网的物联网终端设备时,所述终端设备通信接口模块B(2)与物联网设备串接接口的方式包括设备外设接口、芯片内置插槽,所述网络通信接口模块A(1)与无线通信协议通信接口的方式采用无线通信协议通信接口。

9.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)为芯片。

10.如权利要求1所述的基于通信链路监控对物联网设备进行网络安全防护的方法,其特征在于:所述网络通信链路监控模组(10)具有复用物联网设备核心系统的IP地址功能。

基于通信链路监控对物联网设备进行网络安全防护的方法

【技术领域】

[0001] 本发明涉及网络安全防护的技术领域，特别涉及一种基于通信链路监控对物联网设备进行网络安全防护的方法。

【背景技术】

[0002] 随着物联网产业迅猛发展，其安全也面临着严峻的挑战。特别是物联网设备联网规模激增，加强终端网络安全防护的安全需求也更加紧迫。当前，终端设备的防护思路仍然主要沿用传统互联网安全思维，普遍的做法是基于物联网设备自身的软硬件系统，将适用于互联网终端的认证、防火墙、防病毒、数据加密等技术直接移植到物联网终端系统内，技术思路和防护方法没有针对物联网应用的特点进行设计，不能有效解决以下物联网终端设备的安全防护问题：

[0003] 一、海量终端设备暴露在互联网上，物联网系统的攻击面持续扩大；

[0004] 二、终端设备制造商安全背景不一，设备本身可能存在内置的后门和漏洞，产品及其供应链是否安全缺乏标准参考；

[0005] 三、一些设备自身缺乏安全设计，且在复杂应用环境中面临新安全风险，一旦物联网终端设备系统被攻破，会使整个防护系统失效。要从根本上解决这些问题，需要创新思维，针对物联网应用特点提出新的对终端设备网络通信安全防护的思路。

[0006] 因此，为了有效可行地解决大量物联网设备的网络安全防护问题，有必要提出一种基于通信链路监控对物联网设备进行网络安全防护的方法。

【发明内容】

[0007] 本发明的目的就是解决现有技术中的问题，提出基于通信链路监控对物联网设备进行网络安全防护的方法，能够有效地解决大量物联网设备的网络安全防护问题。

[0008] 为实现上述目的，本发明提出了基于通信链路监控对物联网设备进行网络安全防护的方法，该方法基于一个网络通信链路监控模组，所述网络通信链路监控模组串联在物联网终端设备的网络通信链路上，功能和控制均独立于物联网设备自身的软硬件系统，所述网络通信链路监控模组包括网络通信接口模块A、终端设备通信接口模块B和数据包安全监控模块C，所述数据包安全监控模块C负责对数据包进行合法性判断和处理，所述数据包安全监控模块C通过网络通信接口模块A与网络层通信连接，所述数据包安全监控模块C通过终端设备通信接口模块B与物联网终端设备的核心系统通信连接，该网络安全防护的方法通过以下方式实现：

[0009] 所述网络通信链路监控模组被串联在物联网终端设备与网络层通信的数据链路上，物联网终端设备与网络层的所有通信均需要通过网络通信链路监控模组才能实现，所述数据包安全监控模块C根据内置的规则对经过的数据包进行合法性判断和处理，合法的数据包可透明传输，不合法的数据包被阻截，从而基于通信链路监控对物联网终端设备实现网络通信安全防护功能。

[0010] 作为优选，所述网络通信链路监控模组的数据包安全监控模块C可对经过的数据包进行解析，实施网络通信安全控制策略，所述网络通信安全控制策略包括防火墙、防病毒、入侵检测、身份认证和数据签名、数据包加解密、网络安全态势监测，根据应用场景、所防护物联网终端设备应用特性和安全要求的不同，数据包安全监控模块C的安全控制策略采取上述安全技术中的一种或数种的组合。

[0011] 作为优选，所述网络通信链路监控模组的数据包安全监控模块C可对异常通信数据包进行特征聚类、统计、缓存并通过网络上报至远程安全管理平台，为管理者提供海量的态势采集数据。

[0012] 作为优选，所述网络通信链路监控模组的数据包安全监控模块C还包括管理子模块，所述管理子模块与数据包安全监控模块C通信连接，所述管理子模块具备对数据包处理模块中的处理规则进行设置管理的功能，所述管理子模块通过网络通信接口模块A与远程安全管理平台通信连接。

[0013] 作为优选，所述网络通信链路监控模组还包含配置拔位开关模块，所述配置拔位开关模块与数据包安全监控模块C通信连接并控制数据包安全监控模块C的设置模式，当配置拔位开关模块的开关位于不同开关位时，安全监控模块C的设置模式分别为不允许设置、仅允许本地设置和允许远程设置三种模式。

[0014] 作为优选，所述网络通信链路监控模组还包含本地配置接口模块，所述本地配置接口模块与安全监控模块C通信连接，可对数据包过滤规则、不合规数据包处理和上报规则进行本地设置，所述本地配置接口模块包括但不限于UART接口、SPI接口、IIC接口或SDIO接口。

[0015] 作为优选，所述网络通信链路监控模组的网络通信接口模块A、终端设备通信接口模块B的接口形式包括多种标准有线通信接口，以适用于不同的物联网终端设备有线接入方式。

[0016] 作为优选，所述网络通信链路监控模组用于无线组网的物联网终端设备时，所述终端设备通信接口模块B与物联网设备串接接口的方式包括设备外设接口、芯片内置插槽，所述网络通信接口模块A与无线通信协议通信接口的方式采用无线通信协议通信接口。

[0017] 作为优选，所述网络通信链路监控模组为芯片。

[0018] 作为优选，所述网络通信链路监控模组具有复用物联网设备核心系统的IP地址功能。

[0019] 本发明的有益效果：现有的对物联网终端设备进行网络安全防护的方法，均是基于物联网终端设备自身的软硬件系统，其信任锚基于物联网设备实体。在实际运用中，由于终端设备制造商安全背景不一，难以证明物联网设备实体自身底层软硬件是否安全可信任；物联网终端设备系统应用复杂性也会在应用中引入木马、病毒等不安全的因素。这使得物联网设备实体能否成为网络通信安全的信任锚存在疑问。本发明将信任锚建立在物联网终端设备的网络通信链路上，该安全防护机制独立于物联网应用，不受物联网应用控制，通用性强，安全机制独特：

[0020] 一、安全组网形态使物联网终端设备“隐身”于开放的网络，对其侦察难、攻击难，安全风险被有效隔离，感染传播路径被有效限制，特别是能有效阻止“僵尸网络”的建立和传染；

[0021] 二、基于安全最小化原则，在对各物联网终端设备逐一防护的同时，也为网络安全主管部门提供了海量的网络安全态势监测控制点，对芯片、操作系统、应用层的后门、漏洞实现精准、实时发现，形成持续监测和处置响应能力；

[0022] 三、自身的安全机制简单有效，降低因自身系统复杂而导入新安全风险的可能性，软硬件技术自主可控，从而把安全主动权牢牢掌握在自己手中。

[0023] 本发明的特征及优点将通过实施例结合附图进行详细说明。

【附图说明】

[0024] 图1是本发明的网络通信链路监控模组的框架图；

[0025] 图2是本发明实施例一的方法框架图；

[0026] 图3是本发明实施例二的方法框架图；

[0027] 图4是本发明实施例三的方法框架图；

[0028] 图5是本发明实施例一的方法的流程图。

【具体实施方式】

[0029] 实施例一

[0030] 参阅图1和图2本发明基于通信链路监控对物联网设备进行网络安全防护的方法，该方法基于一个网络通信链路监控模组10，所述网络通信链路监控模组10串联在物联网终端设备的网络通信链路上，功能和控制均独立于物联网设备自身的软硬件系统，所述网络通信链路监控模组10包括网络通信接口模块A1、终端设备通信接口模块B2和数据包安全监控模块C3，所述数据包安全监控模块C3负责对数据包进行合法性判断和处理，所述数据包安全监控模块C3通过网络通信接口模块A1与网络层通信连接，所述数据包安全监控模块C3通过终端设备通信接口模块B2与物联网终端设备的核心系统通信连接，该网络安全防护的方法通过以下方式实现：

[0031] 所述网络通信链路监控模组10被串联在物联网终端设备与网络层通信的数据链路上，物联网终端设备与网络层的所有通信均需要通过网络通信链路监控模组10才能实现，所述数据包安全监控模块C3根据内置的规则对经过的数据包进行合法性判断和处理，合法的数据包可透明传输，不合法的数据包被阻截，从而基于通信链路监控对物联网终端设备实现网络通信安全防护功能，如图5所示。

[0032] 进一步地，所述网络通信链路监控模组10的数据包安全监控模块C3可对经过的数据包进行解析，实施网络通信安全控制策略，所述网络通信安全控制策略包括防火墙、防病毒、入侵检测、身份认证和数据签名、数据包加解密、网络安全态势监测，根据应用场景、所防护物联网终端设备应用特性和安全要求的不同，数据包安全监控模块C3的安全控制策略采取上述安全技术中的一种或数种的组合。所述网络通信链路监控模组10的数据包安全监控模块C3可对异常通信数据包进行特征聚类、统计、缓存并通过网络上报至远程安全管理平台4，为管理者提供海量的态势采集数据。

[0033] 实施例二

[0034] 参阅图3，在实施例一的基础上，所述网络通信链路监控模组10的数据包安全监控模块C3还包括管理子模块31，所述管理子模块31与数据包安全监控模块C3通信连接，所述

管理子模块31具备对数据包处理模块中的处理规则进行设置管理的功能，所述管理子模块31通过网络通信接口模块A1与远程安全管理平台4通信连接。

[0035] 实施例三

[0036] 参阅图4，在实施例二的基础上，所述网络通信链路监控模组10还包含配置拔位开关模块32，所述配置拔位开关模块32与数据包安全监控模块C3通信连接并控制数据包安全监控模块C3的设置模式，当配置拔位开关模块32的开关位于不同开关位时，安全监控模块C3的设置模式分别为不允许设置、仅允许本地设置和允许远程设置三种模式。

[0037] 进一步地，所述网络通信链路监控模组10还包含本地配置接口模块33，所述本地配置接口模块33与安全监控模块C3通信连接，可对数据包过滤规则、不合规数据包处理和上报规则进行本地设置，所述本地配置接口模块包括但不限于UART接口、SPI接口、IIC接口或SDIO接口。所述网络通信链路监控模组10的网络通信接口模块A1、终端设备通信接口模块B2的接口形式包括多种标准有线通信接口，以适用于不同的物联网终端设备有线接入方式。所述网络通信链路监控模组10用于无线组网的物联网终端设备时，所述终端设备通信接口模块B2与物联网设备串接接口的方式包括设备外设接口、芯片内置插槽，所述网络通信接口模块A1与无线通信协议通信接口的方式采用无线通信协议通信接口。

[0038] 进一步地，所述网络通信链路监控模组10为芯片。所述网络通信链路监控模组10具有复用物联网设备核心系统的IP地址功能。

[0039] 本发明将信任锚建立在物联网终端设备的网络通信链路上，该安全防护机制独立于物联网应用，不受物联网应用控制，通用性强，安全机制独特：安全组网形态使物联网终端设备“隐身”于开放的网络，对其侦察难、攻击难，安全风险被有效隔离，感染传播路径被有效限制，特别是能有效阻止“僵尸网络”的建立和传染；基于安全最小化原则，在对各物联网终端设备逐一防护的同时，也为网络安全主管部门提供了海量的网络安全态势监测控制点，对芯片、操作系统、应用层的后门、漏洞实现精准、实时发现，形成持续监测和处置响应能力；自身的安全机制简单有效，降低因自身系统复杂而导入新安全风险的可能性，软硬件技术自主可控，从而把安全主动权牢牢掌握在自己手中。

[0040] 上述实施例是对本发明的说明，不是对本发明的限定，任何对本发明简单变换后的方案均属于本发明的保护范围。

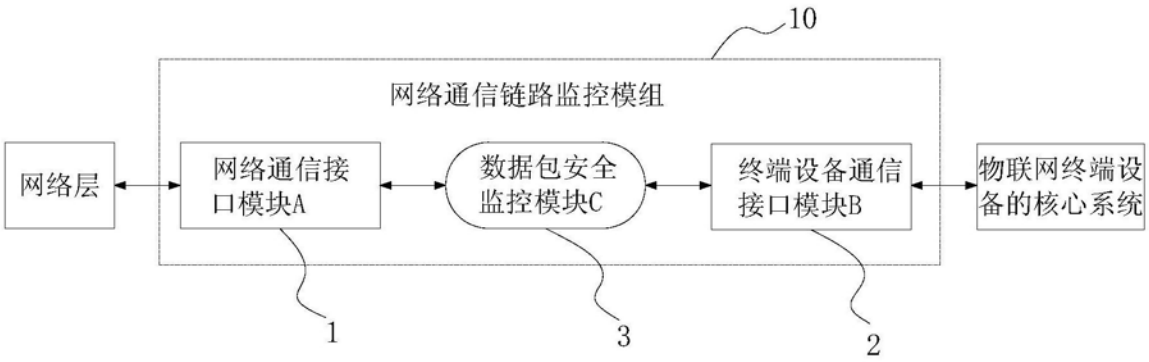

10
网络通信链路监控模组
网络层
网络通信接口模块A
数据包安全监控模块C
终端设备通信接口模块B
物联网终端设备的核心系统
1
3
2

图1

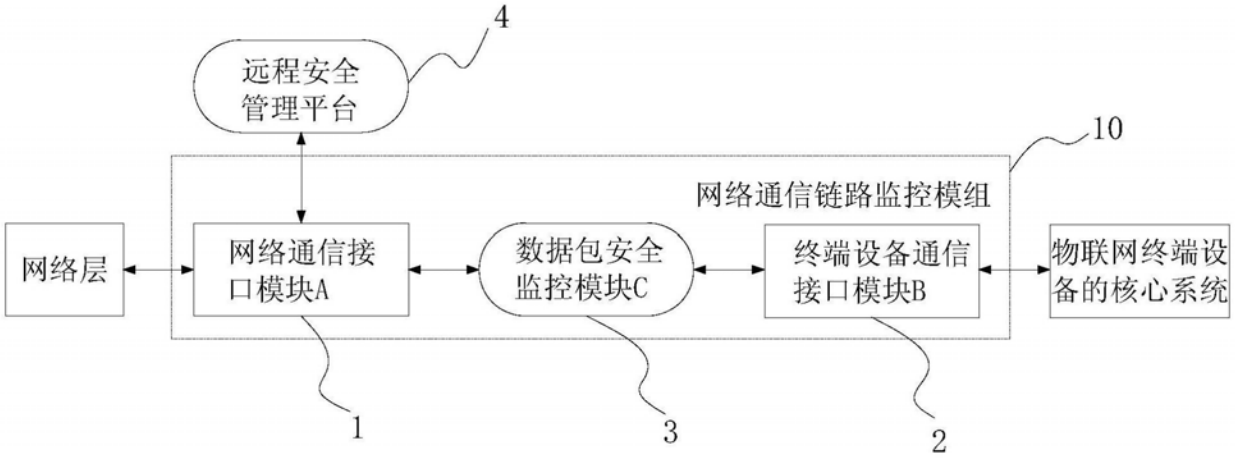

4
远程安全管理平台
10
网络通信链路监控模组
网络层
网络通信接口模块A
数据包安全监控模块C
终端设备通信接口模块B
物联网终端设备的核心系统
1
3
2

图2

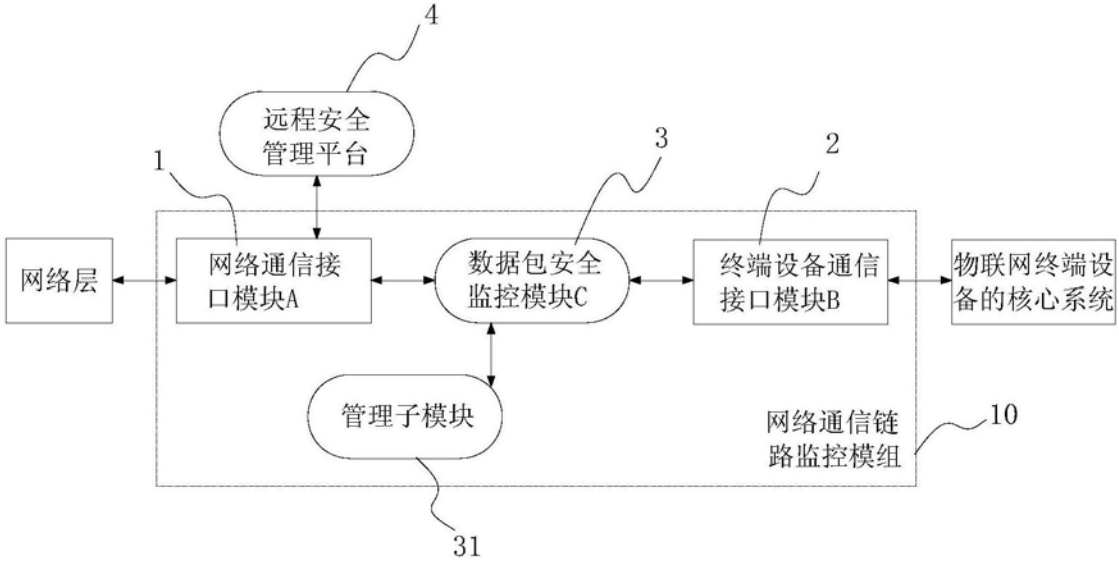

4
远程安全管理平台
1
3
2
网络层
网络通信接口模块A
数据包安全监控模块C
终端设备通信接口模块B
物联网终端设备的核心系统
管理子模块
网络通信链路监控模组
10
31

图3

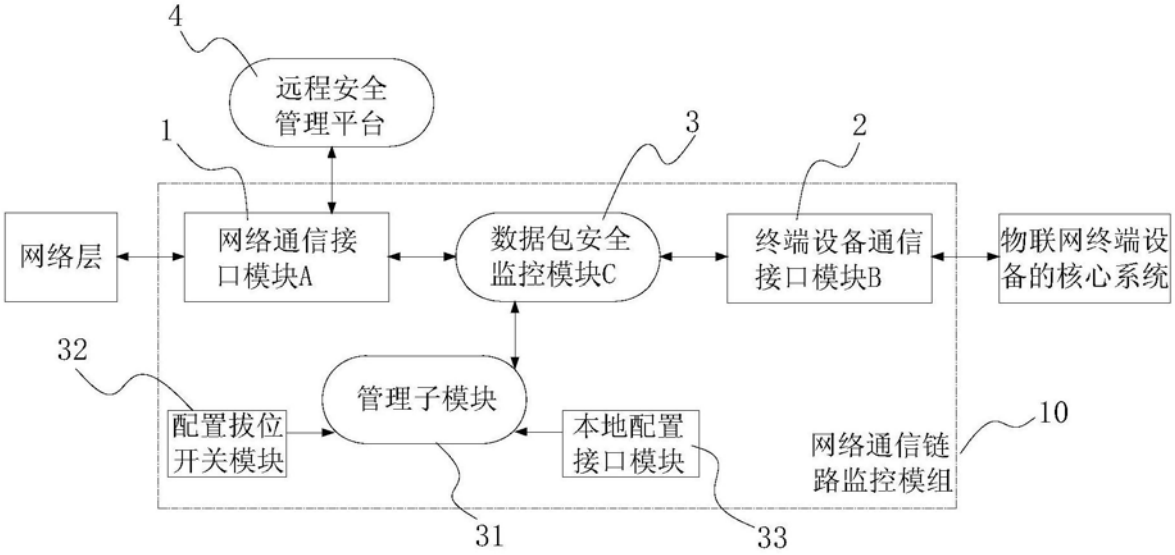

4
远程安全
管理平台
1
3
2
网络层
网络通信接
口模块A
数据包安全
监控模块C
终端设备通信
接口模块B
物联网终端设
备的核心系统
32
管理子模块
配置拔位
开关模块
本地配置
接口模块
网络通信链
路监控模组
10
31
33

图4

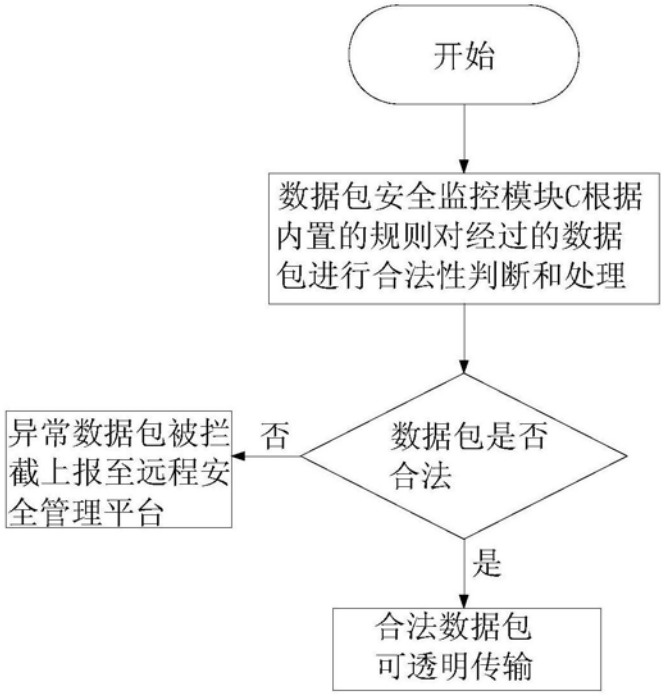

开始
数据包安全监控模块C根据
内置的规则对经过的数据
包进行合法性判断和处理
数据包是否
合法
否
异常数据包被拦
截上报至远程安
全管理平台
是
合法数据包
可透明传输

图5