(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 103139058 A
(43)申请公布日 2013.06.05

(21)申请号 201310032483.9

(22)申请日 2013.01.28

(71)申请人 公安部第一研究所
地址 100048 北京市海淀区首体南路 1 号
申请人 北京中盾安全技术开发公司

(72)发明人 孙论强 李锁雷 苏烈华 李恒训
张凡 秦海权 王国强 尹丹

(74)专利代理机构 北京中海智圣知识产权代理有限公司 11282
代理人 徐金伟

(51)Int.Cl.
H04L 12/66(2006.01)
H04L 29/06(2006.01)

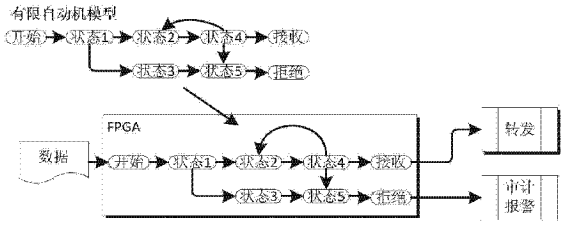
权利要求书1页 说明书9页 附图6页

(54)发明名称

一种物联网安全接入网关

(57)摘要

本发明公开了一种物联网安全接入网关，该网关在硬件层采用 2+1 的三部件架构，即外主机、隔离交换部件、内主机；本发明采用基于硬件的 FPGA 卡作为隔离交换部件，实现网络的隔离和数据的安全、快速交换，并通过内、外主机上的软件层实现设备认证、访问控制、协议解析、数据安全检查、数据摆渡服务和审计服务，使得上述服务的行为可追溯；本发明的优点是能够满足物联网感知终端采集的数据安全导入到核心网内的相关要求，防止通过安全防护比较薄弱的感知层网络向核心网络发起网络攻击、木马病毒传播和拒绝服务攻击，保证了感知网络和核心网络在网络隔离的情况下，实现数据安全交换，在安全得到保障的前提下，满足物联网的实际应用。



CN 103139058 A

1. 一种物联网安全接入网关，其特征在于，包括硬件结构和软件架构，所述硬件结构包括：外主机、隔离交换部件、内主机；所述外主机和所述内主机提供物联网节点的接入控制和数据接入服务；

所述软件架构包括：身份认证模块、访问控制模块；协议解析模块；数据安全检查模块；数据摆渡模块；日志审计模块；用于提供方便的B/S模式的用户接口进行配置管理控制的管理配置模块，所述身份认证模块用于前端感知设备的身份认证和用于执行管理配置模块任何操作之前必须先经过管理员身份鉴别。

2. 根据权利要求1所述的一种物联网安全接入网关，其特征在于，所述隔离交换部件采用基于FPGA芯片开发的双通道隔离交换卡。

3. 根据权利要求2所述的一种物联网安全接入网关，其特征在于，所述双通道隔离交换卡包括PCI和PCI-E两种接口。

4. 根据权利要求1所述的一种物联网安全接入网关，其特征在于，所述身份认证模块包括登陆网关身份认证和感知节点接入设备认证。

5. 根据权利要求4所述的一种物联网安全接入网关，其特征在于，所述登陆网关身份认证是网关自身的身份认证采用双因素方式，即用户名/口令加数字证书，采用数字证书作为身份认证介质。

6. 根据权利要求4所述的一种物联网安全接入网关，其特征在于，所述感知节点接入设备认证用于实现前部件对物联网的感知节点或数据汇集节点进行身份确认，判别是否是合法接入节点。

一种物联网安全接入网关

技术领域

[0001] 本发明涉及一种物联网安全接入网关，属于网络信息交换与安全隔离技术领域。

背景技术

[0002] 目前，传统的安全接入网关主要针对互联网、局域网中实现用户针对特定资源的信息交换、访问控制和行为审计；针对大型网络存在边界不清、安全风险高、纵深防御不足等问题，传统的防火墙等安全防护技术已难支撑，而网闸等设备又面临着成本高，难以适应传感层多协议设备的接入要求、工程实施复杂等问题。并且传统的网关大多是针对 TCP 协议、大数据包，不能针对小包进行优化的。而针对物联网感知数据多为 UDP 协议、64 字节以下的小包居多的情况，功能单一的传统网关已无法进行相应处理。

[0003] 目前，物联网的发展不可避免的伴生着物联网安全问题。物联网感知层的各种业务感知节点和汇聚设备组成感知网络；基于现有的通信网络进行数据传输的网络层和借助网络层进行通信、数据处理、应用的应用层组成核心网络。感知层网络由于其自身技术特点安全防护能力差，安全级别相对于核心网络来说相对较低。物联网安全问题中除了解决各层次中面临的问题以外，不同安全级别的网络之间在保障网络隔离的情况下，如何完成数据的安全交换也是当前存在的技术难题。

发明内容

[0004] 本发明的目的在于提供一种能够克服上述技术问题的物联网安全接入网关，用于解决物联网中感知层网络与核心网络之间在网络隔离的情况下，实现业务数据和控制指令的安全交换。

[0005] 本发明在保证网络隔离的情况下，实现物联网感知网络与核心网络之间的数据安全、快速交换，满足了物联网传感层安全接入的多协议复杂性要求，实现了物联网等大型复杂网络的安全边界控制，体现了“区域防范、纵深防御”以及最小授权的安全原则；以软件能够配置的设备组织形式满足了低成本的要求。本发明在支持大数据包的同时，改进了 FPGA 编程设计，采用有限状态机模型改造 FPGA 程序，使之能够适应物联网数据传输与信息交换的需要。针对不同的前端感知设备采用不同的身份认证方式，包括 USM 方式、Agent 方式和 IP/MAC 绑定方式。

[0006] 本发明综合采用了多种技术，如协议解析、协议检测、内核防护，数据快速摆渡、前端设备认证和数据流向控制等技术；主要包括：

[0007] 1) 传感网络协议库技术；

[0008] 目前中国物联网行业没有形成统一的标准，各个企业、行业在实施物联网项目时，都针对本企业或者行业的需求特征，设计和采用自身需要的物联网产品。因此，物联网传感层协议是五花八门的。

[0009] 物联网安全接入网关必须正确理解和识别各种传感网协议，需要从无到有逐步收集各类物联网产品通信协议，并通过抓包分析、技术交流等各种方式形成知识库，并最终设

计开发一个物联网协议的特征库，使得网关在接收物联网数据时可以识别和理解上述协议，支持主流物联网传感设备接入，使其具有较强的适用性。

[0010] 2) 协议转换技术；

[0011] 在建立物联网协议库后，通过接入网关，将这些不同的协议通过规一化手段转换成核心层标准的应用层协议和统一的数据、信令，从而实现核心层和传感层协议均可以识别的信令和控制指令传递。

[0012] 3) 协议过滤技术；

[0013] 物联网安全接入网关在物联网协议库的基础上，提供对接入数据的协议过滤，针对不同产品的私有协议，对照协议库进行白名单式的过滤，保证接入数据的合法性和正确性。

[0014] 4) 数据高速摆渡技术；

[0015] 当前物联网数据与传统网络数据传输有其自身的特点，表现在 UDP 协议较多，64 字节以下的小包居多的情况。UDP 协议以速度快的优势非常适合物联网使用，并且物联网上传输的绝大多数都是小于 64 字节的小包。而有别于传统网络中传输的 512 或者 1024 字节的大包。

[0016] 5) 前端感知设备的设备身份认证技术；

[0017] 由于物联网所采用的前端感知设备种类众多，而且绝大多数是嵌入式设备。因此传统局域网内的设备认证模式并不适用于物联网。

[0018] 本发明采用多种设备认证模式混合的模式来实现前端感知设备的身份认证，如针对前端感知设备是服务器或者工控机的情况，采用 AGENT 模式，安装软件进行认证；针对前端感知设备是嵌入式设备但支持 SNMP 协议可网管的情况，本发明采用基于 SNMPv3 的模式进行用户名 / 口令认证；针对不可网管的设备，本发明采用 IP/MAC 地址绑定的方式进行设备认证。

[0019] 6) 核心网与传感网的边界控制与安全隔离技术；

[0020] 本发明在传感网的设备中也进行了的相应的设备认证，因此在核心网与传感网间进行网络边界控制并进行安全隔离，能够阻止通过传感网引入的不安全因素。

[0021] 7) 网关操作系统内核加固技术；

[0022] 本发明采用安全操作系统所要求的双因素身份认证登录、最小权限控制、强制访问控制等手段。所述双因素身份认证要求用户采用合法的数字证书，并且输入正确的用户口令才能登录操作系统，最小权限控制保证用户权限分配的合理性。强制访问控制控制只有指定的用户才有权启停网关的各项服务和进程，使用网关的应用文件夹，尽可能缩小超级用户和系统管理员的权限。

[0023] 本发明包括硬件结构和软件架构，本发明的硬件结构采用 2+1 的三部件架构，即包括外主机、隔离交换部件、内主机；所述隔离交换部件采用基于可编程门阵列集成电路（FPGA 芯片）开发的双通道隔离交换卡，实现网络的隔离和数据的安全、快速交换，内、外主机通过部署其上的软件层实现身份认证、访问控制、协议解析、数据安全检查和日志审计，使得上述服务的行为可追溯。

[0024] 本发明的软件架构包括：

[0025] 身份认证模块；

[0026] 访问控制模块；

[0027] 协议解析模块；

[0028] 数据安全检查模块；

[0029] 数据摆渡模块；

[0030] 日志审计模块；

[0031] 管理配置模块，用于提供方便的 B/S 架构的用户接口进行配置管理控制；

[0032] 身份认证模块；所述身份认证模块用于前端感知设备的身份认证和用于执行管理配置模块

[0033] 任何操作之前必须先经过管理员身份鉴别。

[0034] 本发明的外主机、内主机提供物联网节点的接入控制和数据接入服务，隔离交换部件采用基于可编程门阵列集成电路（FPGA 芯片）开发的双通道隔离交换卡（包括 PCI 和 PCI-E 两种接口），实现协议解析、数据摆渡、接入数据流向控制等功能。本发明的外主机、内主机为网关设备提供统一的配置管理界面，实现接入业务的配置、安全策略下发、白名单维护等功能。

[0035] 所述身份认证模块包括登陆网关用户身份认证和感知节点接入设备认证。

[0036] 所述登陆网关用户身份认证采用双因素方式，即用户名 / 口令加数字证书，采用数字证书作为身份认证介质。

[0037] 所述感知节点接入设备认证用于实现前部件对物联网的感知节点或数据汇集节点进行身份确认，判别是否是合法接入节点，包括感知设备（如网络摄像头、RFID 读写器等）的设备认证或接入服务器（如 GPS 定位接入服务器等）的设备认证。

[0038] 所述感知节点接入设备认证方式提供三种模式，根据实际的感知节点适用性来决定采用哪种模式：

[0039] a) AGENT 模式；

[0040] 即由接入网关提供一个 AGENT 程序，提供给各个感知节点设备的生产厂商，在这些设备的硬件中安装此 AGENT 程序，通过 AGENT 的调用，感知节点设备在连接接入网关时，连接信息中带有身份认证信息，接入网关在收到身份认证信息后根据网关中事先设置的记录进行比对，如果比对正确则身份认证成功。并将认证失败的设备加入到阻止列表之中。

[0041] b) USM 认证方式；

[0042] 针对已经存在无法改造的感知设备节点，接入网关通过基于用户的安全模型（user-basedsecurity module:USM）。USM 是 SNMPv3 中采用的新的认证模型，其前提是前端感知设备支持 SNMPv3 可网管。USM 提供了有别于传统用户名 / 口令认证模式中缺少的认证和加密功能。USM 引入了用户名和组的概念，能够设置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间传输的报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合为 NMS 和 Agent 之间的通信提供更高的安全性。

[0043] SNMP 是管理进程（NMS）和代理进程（Agent）之间的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。网络管理员使用 SNMP 功能能够查询设备信息、修改设备的参数值、监控设备状态、自动发现网络故障、生成报告等。通过 SNMP 协议也能够获得前端感知节点的身份信息。

[0044] c)IP/MAC 地址绑定

[0045] 对于不支持 SNMP 协议的前端感知设备，采用 IP/MAC 地址绑定的方式对感知设备进行认证。

[0046] 所述协议解析模块包括协议剥离和重组，其中协议剥离是实现将来自一端网络的数据进行协议解析提取其中的原始数据。协议重组指的是根据对端网络类型，按照一定的协议格式，对完成内容检查的原始数据进行数据重组和协议包装，同时完成相应的地址转换、路由，最后将重组的数据包传入对端网络中，协议解析包括通信协议解析和控制信令解析。

[0047] 协议解析的具体过程如下：

[0048] (1)首先，网关的外部主机将以太网格式剥离，还原 TCP/IP 数据包，发给 IP 层；

[0049] (2)其次，网关的外部主机，剥离 IP 协议，转发 TCP/UDP 包给传输层；

[0050] (3)再次，网关的外部主机，剥离 TCP/UDP 协议。将应用数据转发给第五层；

[0051] (4)最后，网关应用层的代理，进行应用协议的剥离，还原为原始数据；

[0052] (5)如果一个用户访问新浪网，经过网关剥离后的数据，只有 www.sina.com.cn。

[0053] 不同的应用场合，采用的物联网接入网关不尽相同，需要解析的应用协议也不相同，具体如表 1 所示：

[0054] 表 1 接入网关需要解析的协议

[0055]

视频类数据接入网关		
	通信协议解析	➢数据传输协议包括 TCP/IP、RTP/RTCP 等； ➢视频数据编码格式，包括主流的视频编码格式；
	控制协议解析	➢主流摄像头控制协议，如 PELCO-D、PELCO-P、YAAN 等
GPS 类数据接入网关		
	通信协议解析	➢数据传输协议 TCP/IP； ➢GPS 格式数据包；
	控制协议解析	➢常用 GPS 通信协议，如 NEMA 等
RFID 类数据接入网关		
	通信协议解析	➢数据传输协议 TCP/IP； ➢RFID 格式数据包； 具体需要解析的协议包括并不限于：
	控制协议解析	常用 RFID 的控制协议

[0056] 所述数据安全检查模块实现的功能就是协议过滤，所述协议包括数据传输协议和信令控制协议，协议过滤的基础是网关内置物联网协议特征库。

[0057] 通过协议过滤，用户能够确定传感网所传输的数据和信令是合法的，符合网关所

设置的白名单过滤规则，可以接入到核心网。

[0058] 第一步；设定白名单；

[0059] 通过系统设定白名单来控制协议过滤的内容，即明确前端感知设备的品牌厂商，确定其采用的那类协议等；

[0060] 第二步；扫描和分析；

[0061] 其原理是根据所了解的物联网协议特征库，对于所接受的数据严格进行检查和过滤，符合特征库规则的给予放行，否则就直接阻断；

[0062] 第三步接入数据流向控制；

[0063] 在确定接入数据符合协议特征库规则之后，根据白名单所设置的该类接入数据的流向控制规则，确定接入数据流向控制是单向还是双向。

[0064] 接入数据的流向控制逻辑已经固化在FPGA芯片中，比如传输视频数据的UDP包是单向传输的，而传输信令控制协议的TCP包是双向传输的。

[0065] 隔离交换部件根据实现设置的规则，确定某类数据包是只写不读，或者某类数据包是又写又读，这样实现的流向控制功能是由硬件底层完成的，用户不能修改。

[0066] 所述隔离交换部件为保证网络隔离和数据的安全交换采用基于硬件的FPGA隔离卡，所述FPGA隔离卡是感知网络与核心网络之间数据交换的唯一通道，其没有操作系统和应用编程接口，所有的控制逻辑和传输逻辑固化在FPGA芯片中，自主实现数据摆渡。

[0067] FPGA隔离卡主要的特点和技术如下：

[0068] a)主机侧接口采用PCI-Express标准(V1.1)，数据通道宽度为PCI-E×1，保证在该标准下就能实现1Gbit/s的数据通信能力；

[0069] b)隔离卡之间采用了自定义的协议引擎，物理上采用SATA电缆线进行连接；

[0070] c)采用高速串行传输技术(差分线)在PCB上进行高速布板设计，在PCB设计上保证每对差分线是等长，阻抗控制在100欧；

[0071] d)充分利用FPGA的高速吉比特收发器通信能力，采用了CML(CurrentModeLogic)、CDR、线路编码(8B/10B)和预加重等技术，可极大地减小时钟扭曲、信号衰减和线路噪声对接收性能的影响；

[0072] e)自定义协议引擎通过与PFGA高速收发器的配合，形成串并、并串收发器电路，采用的技术有编解码、同步、速率匹配等；

[0073] f)在FPGA内部设计有64KB的发送缓冲区、64KB的接收缓冲区，从而保证主机驱动能最大程度的发挥数据收发的效能，保证在大量小包的收发情况下，仍然具有一个较好的I/O能力；

[0074] g)隔离卡除了纯硬件的设计以外(原理图设计、PCb设计)，在软件编程上采用了Verilog语言对FPGA进行编程，同时该隔离卡在硬件设计上还对FPGA用来加载的程序进行加了密处理。

[0075] 通过对安全检查后的网络数据包进行解析、剥离，还原成原始业务数据，同时在FPGA程序中设定了业务数据传输和信令控制数据传输的不同通道，其中业务数据采用单向传输通道而信令控制数据采用双向传输通道，处理程序固化在FPGA芯片中进行数据分拣。

[0076] 采用专用安全芯片(FPGA芯片)作为隔离交换部件，其具有如下的特点：

[0077] a)硬件独立控制逻辑；

[0078] 芯片本身具有独立控制逻辑，不受任何软系统控制，数据传输不受任何外部信号和指令控制，前后部件只能负责往指定的交换区存放或读写数据，不对传输过程做其他任何控制；

[0079] b) 可靠传输；

[0080] 支持 CRC 校验，保证数据的可靠传输。系统自动进行 CRC 校验，当出现 CRC 校验错时，支持数据重传；

[0081] c) 双摆渡技术；

[0082] 通过硬件控制逻辑隔离交换部件。所述外主机、内主机把需要交换的数据写入或者读出制定的交换区，完成一次摆渡，然后隔离交换部件通过硬件控制逻辑断开与所述外主机、内主机的连接，彼此之间建立连接，自动进行协商，实现数据交换，完成二次摆渡。通过双摆渡技术，内外网络永远不会直接连接，并在此基础上实现内外网络的安全隔离。

[0083] d) 硬件自动协商；

[0084] 隔离交换部件设计有独立控制硬件逻辑，在实现双摆渡技术中，隔离交换部件自动进行协商，数据传输实现硬件互斥访问，按照分时轮询机制实现对连接的自动、高效的控制，防止信号死锁；

[0085] e) 专有协议交换；

[0086] 接入网关只能按照专有的格式进行数据传输。任何数据必须经过分析、过滤，并按照确定的方式进行交换。系统底层实现了专有信息传输，自动完成数据的协议剥离与封装；

[0087] f) 数据分片重组；

[0088] 由于实现了协议和数据的分离，系统只会传递静态纯数据，为了实现用户的透明访问，保障任意大小的数据块都能顺利传输，系统底层自动实现了数据文件按照交换区大小进行自动的分片传输，在系统另一侧，自动按照约定的专有协议进行数据重组，从而实现任意数据的交换；

[0089] g) 实现总线独享，高速流水线操作。无需 CPU 调度，无需总线竞争和申请，每步操作无需等待，实现高效交换。

[0090] h) 接入数据的流向控制；

[0091] 在 FPGA 程序中，设定了业务数据传输和信令控制数据传输的不同通道，其中业务数据采用单向传输通道而信令控制数据采用双向传输通道，处理程序固化在 FPGA 芯片中进行数据分拣。

[0092] 本发明的操作系统安全加固的主要措施是拟采用安全操作系统所要求的管理特权分立、强制访问控制（如主要合法的主体才能访问指定的文件夹或者启停相关进程等）以及内核级安全审计等手段。如下所述：

[0093] a) 管理特权分立；

[0094] 现有操作系统中的应用程序继承用户权限，不满足最小权限原则，从而给病毒等恶意程序留下了破坏系统安全的空间。因此网关允许安全管理员规定执行程序权限，使其在满足用户权限访问控制规则的前提下，只拥有正常完成任务的最小权限。以浏览器程序为例，安全管理员可以配置其只能读那些文件或写那些文件，不允许其访问系统内的重要信息、不允许其修改系统内的关键配置文件，那么即使系统被恶意脚本所攻击，重要信息的

安全性也不会受到威胁，系统本身的完整性也不会受到破坏。

[0095] b) 强制访问控制；

[0096] 现有的操作系统采用自主访问控制模式来限制用户权限，以达到保护系统资源安全的目的。但是在自主访问控制体系中，资源属主可以任意授权，并且权限可以传递，这样不利于信息系统的安全。因此网关增加了强制访问控制机制，由管理中心对系统中的主体（用户、进程）及客体（文件、执行程序、外部设备等）进行安全标识，根据客体类型的不同，分别制定了不同的访问控制规则，从而全方位地保护重要信息，保护信息系统的机密性。

[0097] c) 内核级安全审计；

[0098] 审计数据在系统中应得到严格的保护，防止非授权查看，更要防止数据的篡改和删除，对审计配置文件、审计数据文件实施相应的角色控制，以保证只有审计管理员才能访问。

[0099] 本发明的优点是能够满足物联网感知终端采集的数据安全导入到核心网内的相关要求，防止通过安全防护比较薄弱的感知层网络向核心网络发起网络攻击、木马病毒传播和拒绝服务攻击，保证了感知网络和核心网络在网络隔离的情况下，实现数据安全交换，在安全得到保障的前提下，满足物联网的实际应用。

附图说明

[0100] 图 1 是本发明所述一种物联网安全接入网关的有限状态机模型示意图；

[0101] 图 2 是本发明所述一种物联网安全接入网关的整体架构示意图；

[0102] 图 3 是本发明所述一种物联网安全接入网关的功能示意图；

[0103] 图 4 是本发明所述一种物联网安全接入网关的 Agent 方式的接入设备认证示意图；

[0104] 图 5 是本发明所述一种物联网安全接入网关的协议解析示意图；

[0105] 图 6 是本发明所述一种物联网安全接入网关的基于安全策略数据处理示意图；

[0106] 图 7 是本发明所述一种物联网安全接入网关的管理中心结构示意图；

[0107] 图 8 是本发明所述一种物联网安全接入网关的部署图；

[0108] 图 9 是本发明所述一种物联网安全接入网关的设备到平台部署实施示意图；

[0109] 图 10 是本发明所述一种物联网安全接入网关的系统到平台部署实施示意图。

具体实施方式

[0110] 下面结合附图和实施例对本发明进行详细描述。如图 2 所示，本发明包括硬件结构和软件架构，所述硬件结构包括：外主机、隔离交换部件、内主机；所述外主机和所述内主机提供物联网节点的接入控制和数据接入服务；所述软件架构包括：身份认证模块、访问控制模块；协议解析模块；数据安全检查模块；数据摆渡模块；日志审计模块；用于提供方便的 B/S 用户接口进行配置管理控制的管理配置模块，所述身份认证模块用于前端感知设备的身份认证和执行管理配置模块任何操作之前必须先经过管理员身份鉴别。如图 4 所示，是本发明的采用 Agent 方式进行前端感知设备身份认证示意图。

[0111] 所述隔离交换部件采用基于 FPGA 芯片开发的双通道隔离交换卡。所述双通道隔离交换卡包括 PCI 和 PCI-E 两种接口。

[0112] 本发明采用有线状态机模型改造 FPGA 程序，使之能够适应物联网数据传输的需要，具体如图 1 所示：在利用 FPGA 进行实时数据格式审查时，首先对允许的数据格式和特征以及禁止的特征采用有限状态机建模，并用 FPGA 实现与允许格式和特征相对应的状态机。当数据通过 FPGA 时，数据流在状态机中以流水线方式移动，逐步通过状态机。当数据到达状态机的接收端口时（合法数据），数据被取出，并发送到输出模块。如果数据不符合状态机模型（非法格式或特征），则数据将到达有限状态机的阻截端口，由安全审计报警模块处理，产生阻截和报警操作。

[0113] 由于整个操作是在状态机中以流水线逐步通过，只需要确定的有限的步骤以流水线方式通过，以完成数据的实时审查，因此能够超高速的完成物联网数据的隔离交换。本发明的功能图如图 3 所示。

[0114] 本发明的管理中心向管理用户开发 WEB 服务，管理员通过 HTTPS 方式登录管理中心，进行所有的配置操作、审计日志查询等，本发明的管理中心的框架结构如图 7 所示：

[0115] a) 用户管理子系统；

[0116] 主要负责管理员的添加、修改、删除；管理员的访问权限管理（添加、删除允许访问的服务资源）。

[0117] b) 设备管理子系统；

[0118] 配置系统允许访问的设备资源情况，包括允许访问的地址（或地址范围）。

[0119] c) 服务管理子系统；

[0120] 接入服务的配置管理、服务监控、服务起停等功能。

[0121] d) 主机管理；

[0122] 包括主机 CPU、内存性能监控、网络配置、集中监控上报配置和其他系统参数配置。

[0123] e) 集群配置；

[0124] 主要包括集群节点的管理、双机热备和负载均衡的配置。

[0125] f) 安全审计；

[0126] 系统开机日志、管理员操作日志、内网客户端访问审计、告警日志、传输审计等日志信息的查询、备份管理。

[0127] 本发明的隔离交换部件根据实现设置的规则，确定某类数据包是只写不读，或者某类数据包是又写又读，这样实现的流向控制功能是由硬件底层完成的，用户不能修改。具体检测流程示意图如图 6 所示的基于安全策略数据处理示意图；图 6 中实线表示的是业务数据流，虚线表示的是控制信令流以及感知节点的反馈信息流。来自传输网的数据通过传输协议检测和信令控制协议检测，单向传输到核心网中；同样的，来自核心网的控制信令和反馈信息经过同样的检测之后，可以反向传回传感网。图 5 是本发明的协议解析示意图；

[0128] 本发明部署在感知网络（传感网）与核心网络之间，实现两个网络之间数据的安全交换，具体如图 8 所示。

[0129] 本发明实现了物联网的区域防范，使感知网络的安全风险降至最小。具体实施方案包括两种方式：

[0130] 第一种，前端（即外主机）接入感知设备，例如摄像头、GPS 或者 FRID 设备，后端（即内主机）接入的是系统平台，感知设备通过汇聚节点后，直接将感知数据通过物联网安全接入网关传入到核心网络的应用平台上；具体部署如图 9 所示。

[0131] 第二种，前端（即外主机）接入的为感知设备集成的系统平台，后端（即内主机）接入的是业务应用平台，前端平台将处理后的感知数据通过物联网安全接入网关传入到核心网络的应用平台上；具体部署如图 10 所示。

[0132] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明公开的范围内，能够轻易想到的变化或替换，都应涵盖在本发明权利要求的保护范围内。

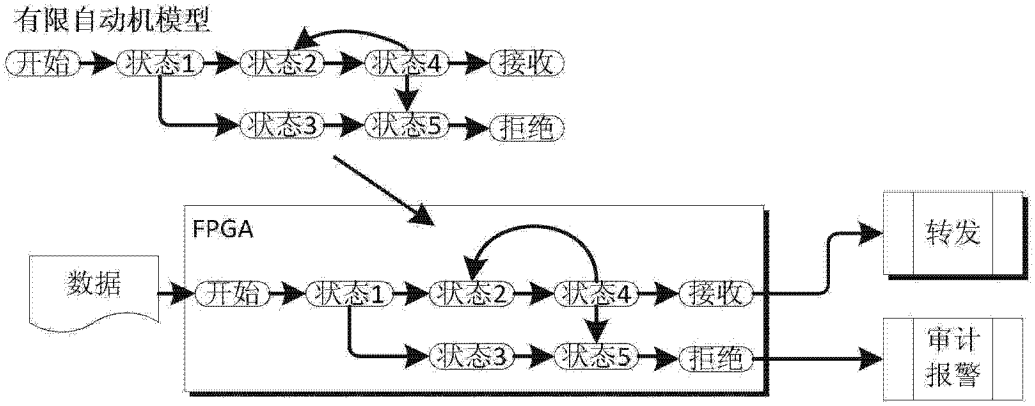

有限自动机模型
开始
状态1
状态2
状态4
接收
状态3
状态5
拒绝
FPGA
数据
开始
状态1
状态2
状态4
接收
状态3
状态5
拒绝
转发
审计
报警

图 1

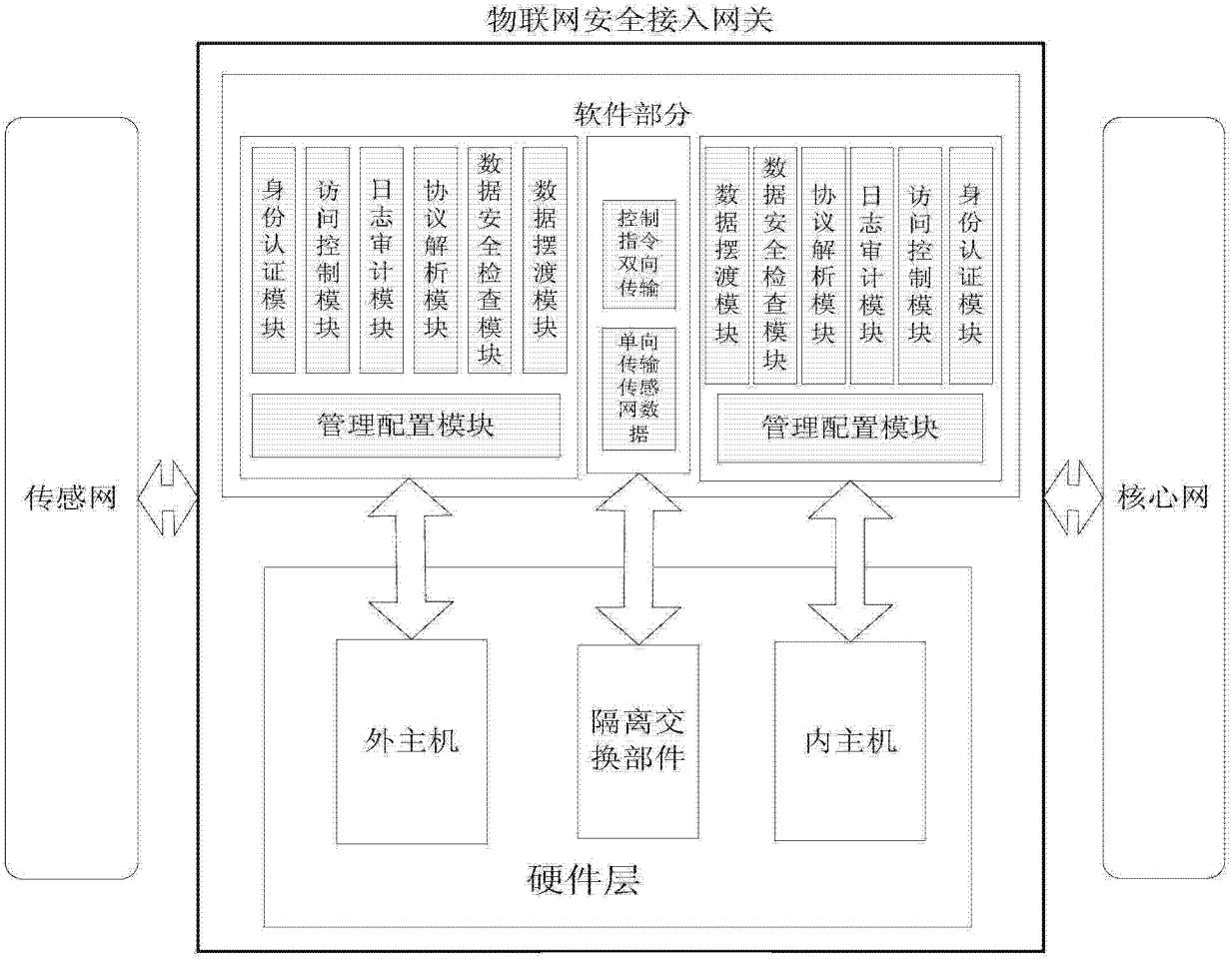

物联网安全接入网关
软件部分
身份认证模块
访问控制模块
日志审计模块
协议解析模块
数据安全检查模块
数据摆渡模块
管理配置模块
控制指令双向传输
单向传输传感网数据
数据摆渡模块
数据安全检查模块
协议解析模块
日志审计模块
访问控制模块
身份认证模块
管理配置模块
传感网
核心网
外主机
隔离交换部件
内主机
硬件层

图 2

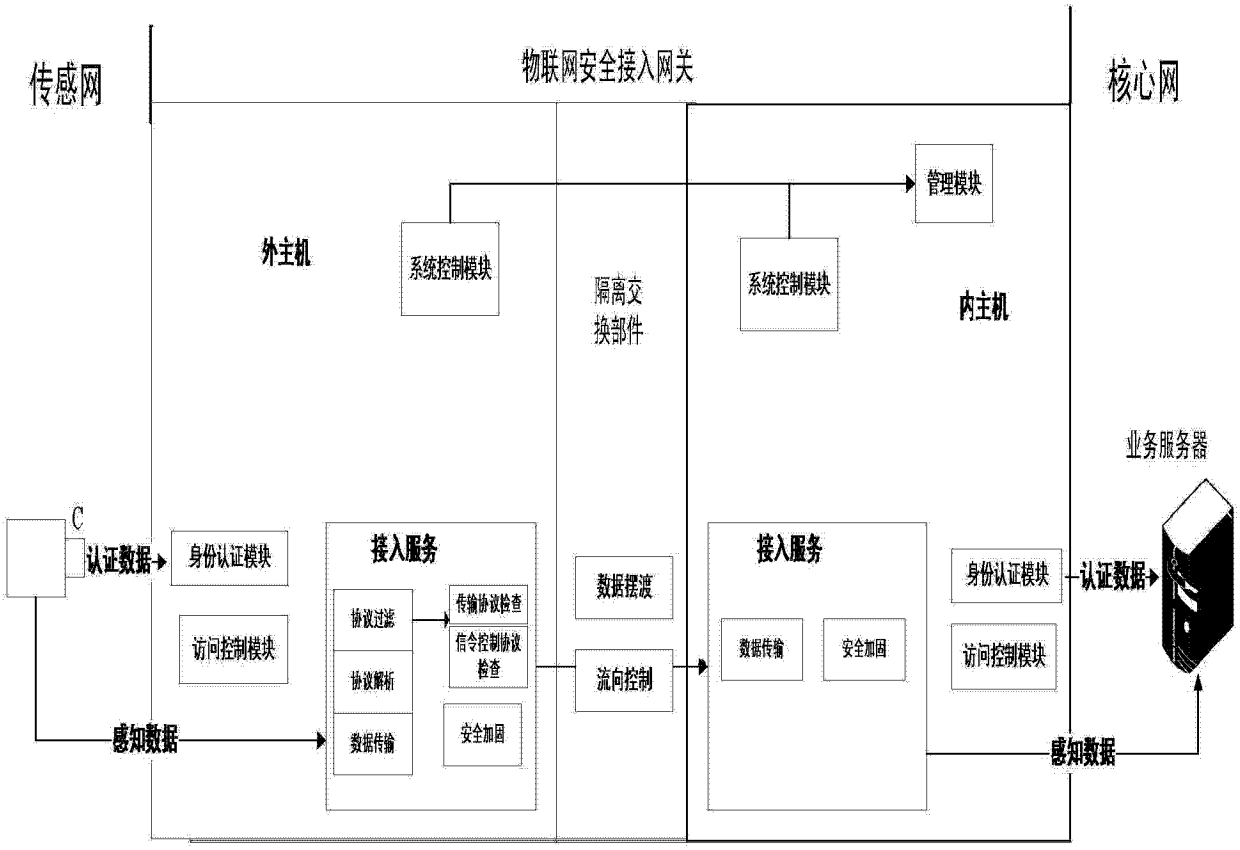

传感网
物联网安全接入网关
核心网
管理模块
外主机
系统控制模块
隔离交换部件
系统控制模块
内主机
业务服务器
C
认证数据
身份认证模块
访问控制模块
接入服务
协议过滤
协议解析
数据传输
传输协议检查
信令控制协议检查
安全加固
数据摆渡
流向控制
接入服务
数据传输
安全加固
身份认证模块
访问控制模块
认证数据
感知数据
感知数据

图 3

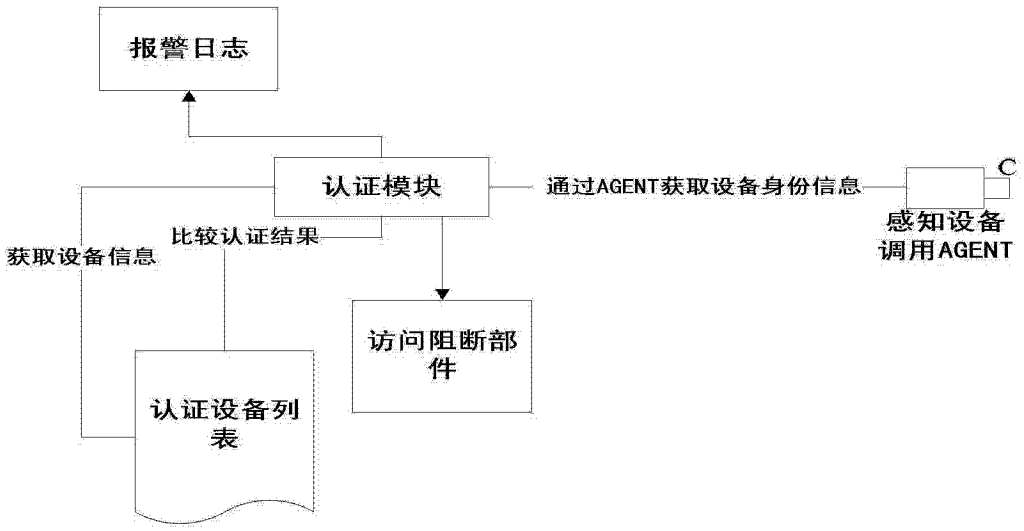

报警日志
认证模块
通过AGENT获取设备身份信息
C
感知设备
调用AGENT
比较认证结果
获取设备信息
访问阻断部件
认证设备列表

图 4

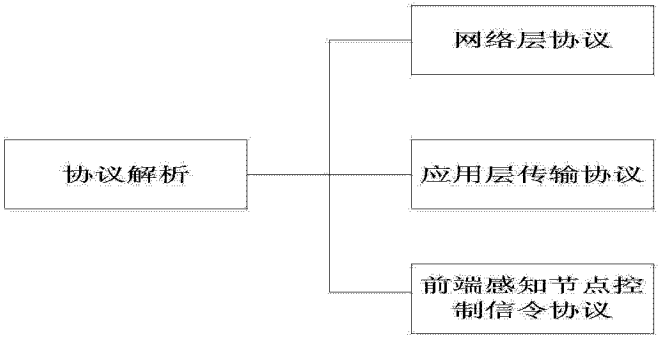

网络层协议
协议解析
应用层传输协议
前端感知节点控制信令协议

图 5

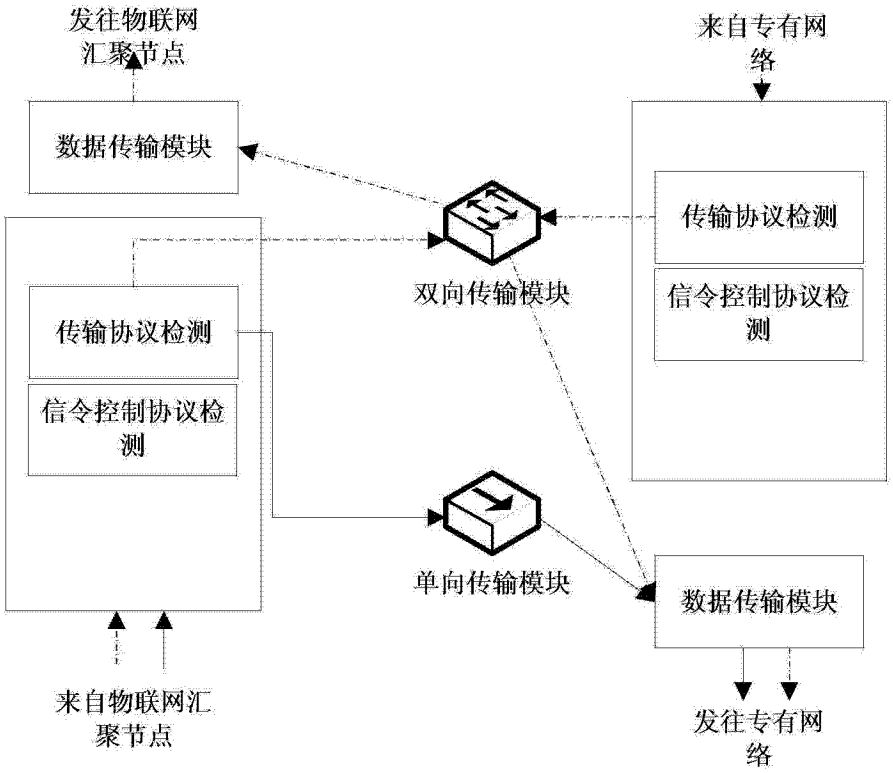

发往物联网汇聚节点
来自专有网络
数据传输模块
传输协议检测
信令控制协议检测
双向传输模块
传输协议检测
信令控制协议检测
单向传输模块
数据传输模块
来自物联网汇聚节点
发往专有网络

图 6

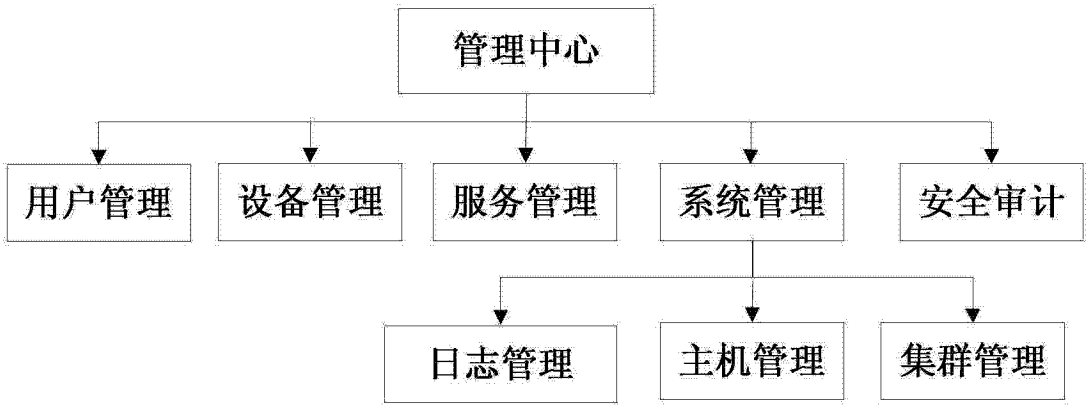


图 7

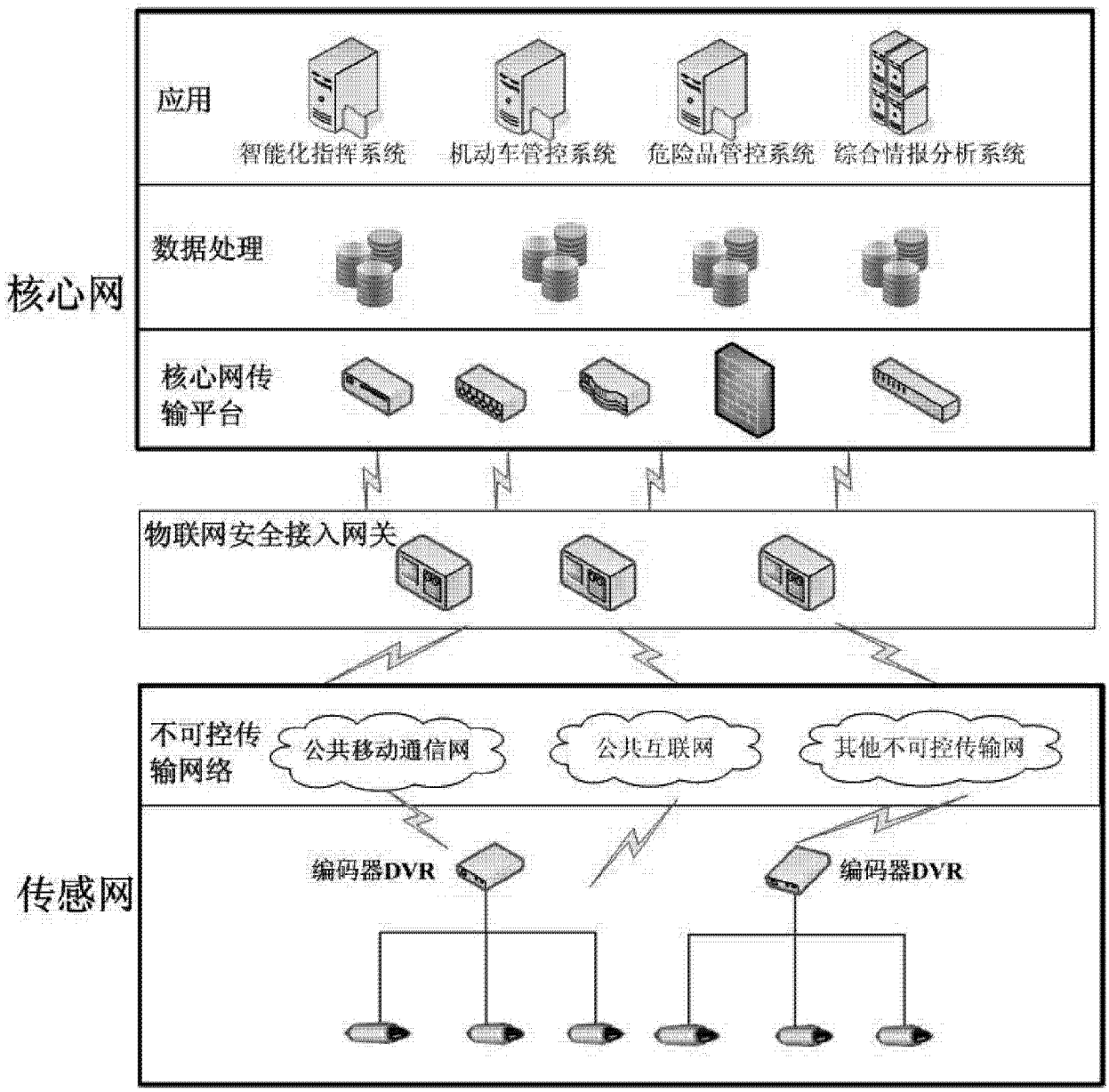

核心网
应用
智能化指挥系统
机动车管控系统
危险品管控系统
综合情报分析系统
数据处理
核心网传输平台
物联网安全接入网关
不可控传输网络
公共移动通信网
公共互联网
其他不可控传输网
传感网
编码器DVR
编码器DVR

图 8

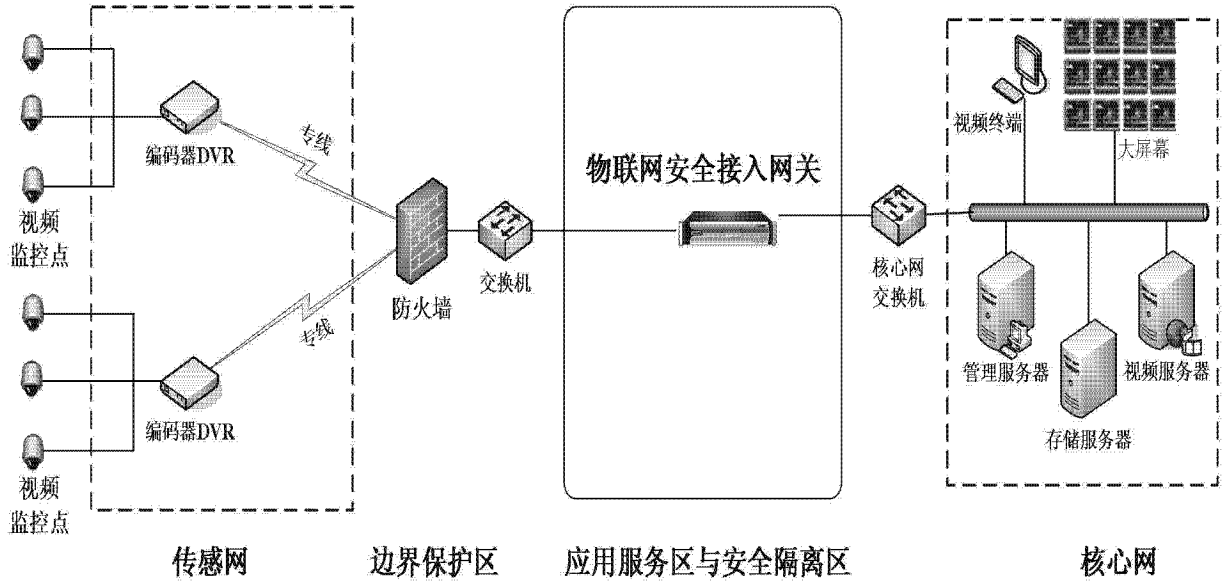

视频
监控点
编码器DVR
专线
视频
监控点
编码器DVR
专线
防火墙
交换机
物联网安全接入网关
核心网
交换机
视频终端
大屏幕
管理服务器
视频服务器
存储服务器
传感网
边界保护区
应用服务区与安全隔离区
核心网

图 9

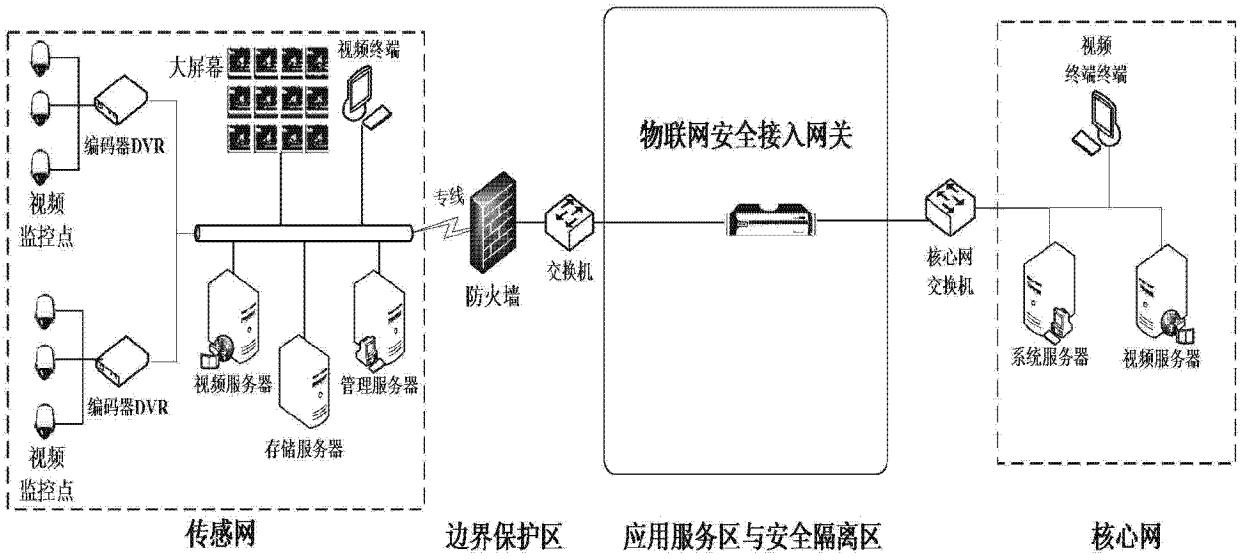

大屏幕
视频终端
编码器DVR
视频
监控点
编码器DVR
视频
监控点
视频服务器
管理服务器
存储服务器
专线
防火墙
交换机
物联网安全接入网关
核心网
交换机
视频
终端终端
系统服务器
视频服务器
传感网
边界保护区
应用服务区与安全隔离区
核心网

图 10