



(21) 申请号 202411710663.2

(22) 申请日 2024.11.27

(71) 申请人 杭州瑞盛电气有限公司

地址 310000 浙江省杭州市临安区锦城街
道新溪桥村新溪桥135号

(72) 发明人 余永辉 邢昇凯 谢晓燕

(74) 专利代理机构 北京华夏博通专利事务所

(普通合伙) 11264

专利代理师 熊敬

(51) Int. Cl.

H04L 67/10 (2022.01)

H04L 67/125 (2022.01)

H04L 9/40 (2022.01)

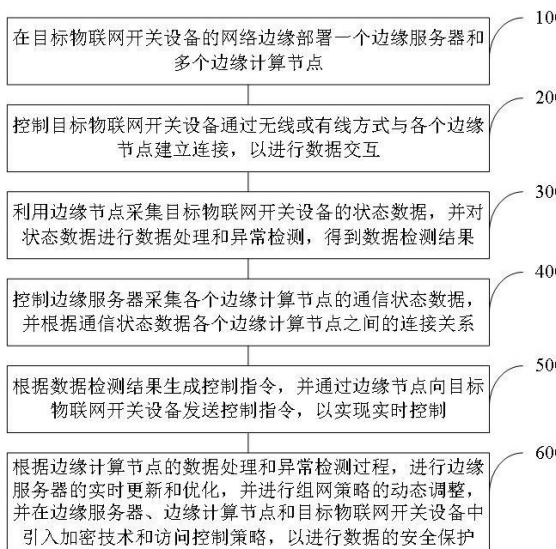
权利要求书3页 说明书9页 附图1页

(54) 发明名称

一种基于边缘计算的物联网开关控制方法及系统

(57) 摘要

本发明提供了一种基于边缘计算的物联网开关控制方法及系统,涉及物联网技术领域,在目标物联网开关设备的网络边缘部署边缘装置,实现与设备的数据交互。边缘节点负责采集设备的状态数据,并进行数据处理和异常检测;边缘服务器收集各个边缘计算节点的通信状态数据,分析节点之间的连接关系;根据数据检测结果生成控制指令并实时发送至目标物联网开关设备;同时边缘服务器根据数据处理和异常检测的反馈进行实时更新和优化,动态调整网络策略;引入加密技术和访问控制策略,保护数据传输和存储的安全性。本发明通过降低延迟、提高处理效率、增强安全性和可靠性,该方法能够有效适应现代智能化应用的需求,提升物联网系统的整体性能。



1. 一种基于边缘计算的物联网开关控制方法,其特征在于,包括:

在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点;

控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接,以进行数据交互;

利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据处理和异常检测,得到数据检测结果;

控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系;

根据所述数据检测结果生成控制指令,并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令,以实现实时控制;

根据所述边缘计算节点的数据处理和异常检测过程,进行所述边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。

2. 根据权利要求1所述的基于边缘计算的物联网开关控制方法,其特征在于,利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据处理和异常检测,得到数据检测结果,包括:

基于预设的通信协议,通过所述边缘节点实时采集目标物联网开关设备的状态数据;所述状态数据包括:电流信号、电压信号、设备状态信号、温度信号、设备所在环境信号、以及各个信号对应的时间序列信号;

对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号;

对所述电流信号、电压信号、设备状态信号、温度信号和设备所在环境信号进行标准化处理,得到标准信号;

对所述标准信号进行去噪处理,得到去噪信号;

对所述去噪信号及对应的所述简化序列信号进行特征提取,得到异常特征;

将所述异常特征输入至训练好的设备异常状态检测模型中,得到所述数据检测结果。

3. 根据权利要求2所述的基于边缘计算的物联网开关控制方法,其特征在于,对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号,包括:

基于公式
$$v_i^{(\tau)} = \frac{1}{\tau} \sum_{b=(i-1)\tau+1}^{i\tau} x_b, 1 \leq i \leq \left\lceil \frac{N_0}{\tau} \right\rceil$$
 对所述时间序列信号进行粗粒

化处理,得到粗粒化序列;其中, $v_i^{(\tau)}$ 为预设的自适应尺度因子 τ 下粗粒化序列的第 i 个数

据, x_b 为所述时间序列信号中第 b 个数据点, $b \in [1, N_0]$, N_0 为时间序列长度, $\left\lceil \frac{N_0}{\tau} \right\rceil$ 为

粗粒化序列的数据个数,自适应尺度因子 τ 的计算公式为: $\tau = \frac{\sigma}{\mu} \times k$, σ 为时间序列的标

准差, μ 为时间序列的均值, k 为目标物联网开关设备的预设经验常数;

将所述粗粒化序列分配到从0到1的区间内,得到分配后的序列;

将所述分配后的序列映射到1到 $N+$ 之间的整数,得到所述简化序列信号; $N+$ 为大于1的

整数。

4. 根据权利要求2所述的基于边缘计算的物联网开关控制方法,其特征在于,对所述标准信号进行去噪处理,得到去噪信号,包括:

对所述标准信号进行平移,得到平移后的信号;

对所述平移后的信号进行小波分解,得到多个小波系数;

根据信号的分解尺度和长度确定滤波阈值;

根据所述滤波阈值构建去噪函数;

利用所述去噪函数去除所述平移后的信号的噪声,得到初步的去噪信号;

采用移动平均法对所述初步的去噪信号进行信号平滑,并通过信噪比和均方误差的指标评估去噪效果,以确定最终的去噪信号。

5. 根据权利要求4所述的基于边缘计算的物联网开关控制方法,其特征在于,所述滤波

阈值的计算公式为:
$$\begin{cases} W_j = \frac{\text{median}(|d_j|)}{0.6745} \sqrt{2 \log N} \\ \lambda = W_j / \log(j+1) \end{cases}$$
; 其中, λ 为滤波阈值, j 为平移后的信号

的分解尺度, d_j 为分解尺度为 j 的小波系数, N 表示平移后的信号的长度, median 表示取中值运算。

6. 根据权利要求2所述的基于边缘计算的物联网开关控制方法,其特征在于,所述异常特征包括:信号的时间域特征、频域特征和时序特征。

7. 根据权利要求1所述的基于边缘计算的物联网开关控制方法,其特征在于,控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系,包括:

利用边缘服务器周期性获取各所述边缘计算节点及其周围预设距离范围内的边缘计算节点的通信状态信息;各所述边缘计算节点构成一个用于通信交互的拓扑网络结构;

将获取的通信状态信息输入到预先建立的节点连接决策模型中,得到实时决策结果;

基于实时决策结果,实时动态调整拓扑网络结构中各边缘计算节点和周围预设距离范围内的边缘计算节点的连接关系,形成自适应的拓扑网络结构;所述实时决策结果中包括拓扑网络结构中各边缘计算节点需要连接和需要断开的边缘计算节点。

8. 根据权利要求1所述的基于边缘计算的物联网开关控制方法,其特征在于,所述通信状态信息包括信号强度、数据传输速率、丢包率、延迟、能耗、移动速度和历史连接质量中至少一项。

9. 根据权利要求1所述的基于边缘计算的物联网开关控制方法,其特征在于,在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护,包括:

采用端到端加密技术和同态加密算法进行数据加密,并采用区块链技术进行加密数据的存储;

根据用户角色分配访问权限,并结合生物特征和行为特征,提供网络访问的多种认证方式;

结合WiFi探针技术,在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设

备上采集性能指标进行性能监控。

10.一种基于边缘计算的物联网开关控制系统,其特征在于,包括:

部署模块,用于在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点;

连接模块,用于控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接,以进行数据交互;

数据处理模块,用于利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据处理和异常检测,得到数据检测结果;

计算模块,用于控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系;

控制模块,用于根据所述数据检测结果生成控制指令,并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令,以实现实时控制;

保护模块,用于根据所述边缘计算节点的数据处理和异常检测过程,进行所述边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。

一种基于边缘计算的物联网开关控制方法及系统

技术领域

[0001] 本发明涉及物联网技术技术领域,特别是涉及一种基于边缘计算的物联网开关控制方法及系统。

背景技术

[0002] 随着物联网 (IoT) 的快速发展,连接到网络的智能设备数量呈爆炸式增长。传统的云计算模式需要将大量数据上传至云端进行处理,存在以下问题:

(1) 高延迟,数据传输和处理需要时间,无法满足实时性要求。

[0003] (2) 高带宽消耗,大量数据上传占用网络带宽,可能导致网络拥堵。

[0004] (3) 安全风险,数据在传输过程中可能被拦截、篡改,存在安全隐患。

[0005] 边缘计算作为一种新兴的计算模式,通过在网络边缘处理数据,可以有效降低延迟、节省带宽并提高安全性。然而,现有的物联网开关控制方法大多未充分利用边缘计算的优势,无法满足高效、安全的控制需求。

发明内容

[0006] 为了克服现有技术的不足,本发明的目的是提供一种基于边缘计算的物联网开关控制方法及系统,通过降低延迟、提高处理效率、增强安全性和可靠性等多方面的优势,能够有效提升物联网系统的整体性能和用户体验,适应现代智能化应用的需求。

[0007] 为实现上述目的,本发明提供了如下方案:

一种基于边缘计算的物联网开关控制方法,包括:

在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点;

控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接,以进行数据交互;

利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据分析和异常检测,得到数据检测结果;

控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系;

根据所述数据检测结果生成控制指令,并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令,以实现实时控制;

根据所述边缘计算节点的数据处理和异常检测过程,进行所述边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。

[0008] 优选地,利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据分析和异常检测,得到数据检测结果,包括:

基于预设的通信协议,通过所述边缘节点实时采集目标物联网开关设备的状态数据;所述状态数据包括:电流信号、电压信号、设备状态信号、温度信号、设备所在环境信号、

以及各个信号对应的时间序列信号；

对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号；

对所述电流信号、电压信号、设备状态信号、温度信号和设备所在环境信号进行标准化处理,得到标准信号；

对所述标准信号进行去噪处理,得到去噪信号；

对所述去噪信号及对应的所述简化序列信号进行特征提取,得到异常特征；

将所述异常特征输入至训练好的设备异常状态检测模型中,得到所述数据检测结果。

[0009] 优选地,对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号,包括:

基于公式 $\mathbf{v}_i^{(\tau)} = \frac{1}{\tau} \sum_{b=(i-1)\tau+1}^{i\tau} \mathbf{x}_b, 1 \leq i \leq \left\lceil \frac{N_0}{\tau} \right\rceil$ 对所述时间序列信号进行

粗粒化处理,得到粗粒化序列;其中, $\mathbf{v}_i^{(\tau)}$ 为预设的自适应尺度因子 τ 下粗粒化序列的第 i

个数据, $\mathbf{x}_b$ 为所述时间序列信号中第 b 个数据点, $b \in [1, N_0]$, N_0 为时间序列长度,

$\left\lceil \frac{N_0}{\tau} \right\rceil$ 为粗粒化序列的数据个数,自适应尺度因子 τ 的计算公式为: $\tau = \frac{\sigma}{\mu} \times k$, σ 为时间序列

的标准差, μ 为时间序列的均值, k 为目标物联网开关设备的预设经验常数;

将所述粗粒化序列分配到从0到1的区间内,得到分配后的序列;

将所述分配后的序列映射到1到 $N+$ 之间的整数,得到所述简化序列信号; $N+$ 为大于1的整数。

[0010] 优选地,对所述标准信号进行去噪处理,得到去噪信号,包括:

对所述标准信号进行平移,得到平移后的信号;

对所述平移后的信号进行小波分解,得到多个小波系数;

根据信号的分解尺度和长度确定滤波阈值;

根据所述滤波阈值构建去噪函数;

利用所述去噪函数去除所述平移后的信号的噪声,得到初步的去噪信号;

采用移动平均法对所述初步的去噪信号进行信号平滑,并通过信噪比和均方误差的指标评估去噪效果,以确定最终的去噪信号。

[0011] 优选地,所述滤波阈值的计算公式为:
$$\begin{cases} W_j = \frac{\text{median}(|d_j|)}{0.6745} \sqrt{2 \log N} \\ \lambda = W_j / \log(j+1) \end{cases}$$
 ;其中, λ 为滤

波阈值, j 为平移后的信号的分解尺度, d_j 为分解尺度为 j 的小波系数, N 表示平移后的信号的长度, median 表示取中值运算。

[0012] 优选地,所述异常特征包括:信号的时间域特征、频域特征和时序特征。

[0013] 优选地,控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系,包括:

利用边缘服务器周期性获取各所述边缘计算节点及其周围预设距离范围内的边

缘计算节点的通信状态信息；各所述边缘计算节点构成一个用于通信交互的拓扑网络结构；

将获取的通信状态信息输入到预先建立的节点连接决策模型中，得到实时决策结果；

基于实时决策结果，实时动态调整拓扑网络结构中各边缘计算节点和周围预设距离范围内的边缘计算节点的连接关系，形成自适应的拓扑网络结构；所述实时决策结果中包括拓扑网络结构中各边缘计算节点需要连接和需要断开的边缘计算节点。

[0014] 优选地，所述通信状态信息包括信号强度、数据传输速率、丢包率、延迟、能耗、移动速度和历史连接质量中至少一项。

[0015] 优选地，在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略，以进行数据的安全保护，包括：

采用端到端加密技术和同态加密算法进行数据加密，并采用区块链技术进行加密数据的存储；

根据用户角色分配访问权限，并结合生物特征和行为特征，提供网络访问的多种认证方式；

结合WiFi探针技术，在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备上采集性能指标进行性能监控。

[0016] 一种基于边缘计算的物联网开关控制系统，包括：

部署模块，用于在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点；

连接模块，用于控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接，以进行数据交互；

数据处理模块，用于利用边缘节点采集所述目标物联网开关设备的状态数据，并对所述状态数据进行数据处理和异常检测，得到数据检测结果；

计算模块，用于控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据，并根据所述通信状态数据各个所述边缘计算节点之间的连接关系；

控制模块，用于根据所述数据检测结果生成控制指令，并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令，以实现实时控制；

保护模块，用于根据所述边缘计算节点的数据处理和异常检测过程，进行所述边缘服务器的实时更新和优化，并进行组网策略的动态调整，并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略，以进行数据的安全保护。

[0017] 根据本发明提供的具体实施例，本发明公开了以下技术效果：

本发明提供了一种基于边缘计算的物联网开关控制方法及系统，方法包括：在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点；控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接，以进行数据交互；利用边缘节点采集所述目标物联网开关设备的状态数据，并对所述状态数据进行数据处理和异常检测，得到数据检测结果；控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据，并根据所述通信状态数据各个所述边缘计算节点之间的连接关系；根据所述数据检测结果生

成控制指令,并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令,以实现实时控制;根据所述边缘计算节点的数据处理和异常检测过程,进行所述边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。本发明通过降低延迟、提高处理效率、增强安全性和可靠性等多方面的优势,能够有效提升物联网系统的整体性能和用户体验,适应现代智能化应用的需求。

附图说明

[0018] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0019] 图1为本发明实施例提供的方法流程图。

具体实施方式

[0020] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0021] 本发明的目的是提供一种基于边缘计算的物联网开关控制方法及系统,通过降低延迟、提高处理效率、增强安全性和可靠性等多方面的优势,能够有效提升物联网系统的整体性能和用户体验,适应现代智能化应用的需求。

[0022] 为使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0023] 图1为本发明实施例提供的方法流程图,如图1所示,本发明提供了一种基于边缘计算的物联网开关控制方法,包括:

步骤100:在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点;

步骤200:控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接,以进行数据交互;

步骤300:利用边缘节点采集目标物联网开关设备的状态数据,并对状态数据进行数据处理和异常检测,得到数据检测结果;

步骤400:控制边缘服务器采集各个边缘计算节点的通信状态数据,并根据通信状态数据各个边缘计算节点之间的连接关系;

步骤500:根据数据检测结果生成控制指令,并通过边缘节点向目标物联网开关设备发送控制指令,以实现实时控制;

步骤600:根据边缘计算节点的数据处理和异常检测过程,进行边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在边缘服务器、边缘计算节点和目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。

[0024] 优选地,利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据处理和异常检测,得到数据检测结果,包括:

基于预设的通信协议,通过所述边缘节点实时采集目标物联网开关设备的状态数据;所述状态数据包括:电流信号、电压信号、设备状态信号、温度信号、设备所在环境信号、以及各个信号对应的时间序列信号;

对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号;

对所述电流信号、电压信号、设备状态信号、温度信号和设备所在环境信号进行标准化处理,得到标准信号;示范性的,本实施例的标准化处理过程是将不同量纲的数据标准化,以便于后续处理。

[0025] 对所述标准信号进行去噪处理,得到去噪信号;

对所述去噪信号及对应的所述简化序列信号进行特征提取,得到异常特征;

将所述异常特征输入至训练好的设备异常状态检测模型中,得到所述数据检测结果。

[0026] 优选地,对所述时间序列信号进行粗粒化和映射处理,得到简化序列信号,包括:

基于公式 $\mathbf{v}_i^{(\tau)} = \frac{1}{\tau} \sum_{b=(i-1)\tau+1}^{i\tau} \mathbf{x}_b, 1 \leq i \leq \left\lfloor \frac{N_0}{\tau} \right\rfloor$ 对所述时间序列信号进行

粗粒化处理,得到粗粒化序列;其中, $\mathbf{v}_i^{(\tau)}$ 为预设的自适应尺度因子 τ 下粗粒化序列的第 i

个数据, $\mathbf{x}_b$ 为所述时间序列信号中第 b 个数据点, $b \in [1, N_0]$, N_0 为时间序列长度,

$\left\lfloor \frac{N_0}{\tau} \right\rfloor$ 为粗粒化序列的数据个数,自适应尺度因子 τ 的计算公式为: $\tau = \frac{\sigma}{\mu} \times k$, σ 为时间序列

的标准差, μ 为时间序列的均值, k 为目标物联网开关设备的预设经验常数;

将所述粗粒化序列分配到从0到1的区间内,得到分配后的序列;

将所述分配后的序列映射到1到 $N+$ 之间的整数,得到所述简化序列信号; $N+$ 为大于1的整数。

[0027] 进一步地,本实施例通过分析历史数据,观察在特定条件下设备运行时的信号波动情况,确定一个合适的 k 值。本实施例通过统计分析设备在正常工作状态下的标准差和均值,选择一个使得粗粒化后信号仍能有效反映设备状态的 k 值;此外,本实施例还可分析时间序列信号的分布特征(如正态分布、偏态分布等),选择适合该分布的 k 值,以确保在粗粒化后信号的代表性。示范性的,在高噪声环境中,本实施例建议将 k 的值设置为1.5到2.5,以确保在粗粒化过程中能够有效过滤掉噪声;对于工业环境中的开关设备, k 的值可以在1.0到3.0 之间。工业设备通常面临更大的负载和环境变化,因此需要更大的 k 值来适应信号的波动。对于家庭环境中的智能开关设备, k 的值通常在0.5到1.5之间。这是因为家庭设备的信号波动相对较小,选择较小的 k 值可以更好地捕捉到设备状态的变化。

[0028] 具体的,本实施例对时间序列进行粗粒化处理有多种好处,包括以下几个方面:

1、减少数据量,粗粒化可以显著降低数据的存储和处理需求,尤其是在处理大规模时间序列数据时。通过减少数据点的数量,可以节省存储空间和计算资源。

[0029] 2、提高计算效率,处理较少的数据点通常意味着更快的计算速度。这对于实时数

据处理和分析非常重要,尤其是在边缘计算或资源受限的环境中。

[0030] 优选地,对所述标准信号进行去噪处理,得到去噪信号,包括:

对所述标准信号进行平移,得到平移后的信号;

对所述平移后的信号进行小波分解,得到多个小波系数;

根据信号的分解尺度和长度确定滤波阈值;

根据所述滤波阈值构建去噪函数;

利用所述去噪函数去除所述平移后的信号的噪声,得到初步的去噪信号;

采用移动平均法对所述初步的去噪信号进行信号平滑,并通过信噪比和均方误差的指标评估去噪效果,以确定最终的去噪信号。

[0031] 优选地,所述滤波阈值的计算公式为:
$$\begin{cases} W_j = \frac{\text{median}(|d_j|)}{0.6745} \sqrt{2 \log N} \\ \lambda = W_j / \log(j+1) \end{cases}$$
; 其中, λ 为滤波

波阈值, j 为平移后的信号的分解尺度, d_j 为分解尺度为 j 的小波系数, N 表示平移后的信号的长度, median 表示取中值运算。

[0032] 优选地,所述异常特征包括:信号的时间域特征、频域特征和时序特征。

[0033] 具体的,本实施例的异常特征主要包括:

1、时间域特征

(1) 均值 (Mean), 信号在一定时间窗口内的平均值,反映了信号的整体水平。

[0034] (2) 标准差 (Standard Deviation), 信号的波动程度,较大的标准差可能表示信号存在异常波动。

[0035] (3) 最大值和最小值 (Max/Min), 信号的最大和最小值,异常状态可能对应于超出正常范围的极值。

[0036] (4) 峰度 (Kurtosis), 描述信号分布的尖锐程度,较高的峰度可能表示信号存在异常变化。

[0037] (5) 偏度 (Skewness), 描述信号分布的对称性,偏度的变化可能指示信号的异常行为。

[0038] 2、频域特征

(1) 频谱特征,通过傅里叶变换得到的频谱,分析信号的频率成分,异常频率成分可能指示设备故障。

[0039] (2) 主频 (Dominant Frequency), 信号中最显著的频率,通常与设备的正常工作频率相关,偏离正常频率可能表示异常。

[0040] (3) 频带能量 (Band Energy), 在特定频带内的能量分布,异常能量集中可能指示设备的异常状态。

[0041] 3、时序特征

(1) 信号的变化率 (Rate of Change), 信号在单位时间内的变化速率,异常的快速变化可能指示故障。

[0042] (2) 异常点检测 (Anomaly Points), 在时间序列中检测到的异常点或突变,通常通过统计方法或机器学习模型识别。

[0043] 优选地,控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系,包括:

利用边缘服务器周期性获取各所述边缘计算节点及其周围预设距离范围内的边缘计算节点的通信状态信息;各所述边缘计算节点构成一个用于通信交互的拓扑网络结构;

将获取的通信状态信息输入到预先建立的节点连接决策模型中,得到实时决策结果;

基于实时决策结果,实时动态调整拓扑网络结构中各边缘计算节点和周围预设距离范围内的边缘计算节点的连接关系,形成自适应的拓扑网络结构;所述实时决策结果中包括拓扑网络结构中各边缘计算节点需要连接和需要断开的边缘计算节点。

[0044] 优选地,所述通信状态信息包括信号强度、数据传输速率、丢包率、延迟、能耗、移动速度和历史连接质量中至少一项。

[0045] 优选地,在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护,包括:

采用端到端加密技术和同态加密算法进行数据加密,并采用区块链技术进行加密数据的存储;

根据用户角色分配访问权限,并结合生物特征和行为特征,提供网络访问的多种认证方式;

结合WiFi探针技术,在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备上采集性能指标进行性能监控。

[0046] 具体的,首先,本实施例的数据加密采用端到端加密技术,确保数据在传输过程中始终处于加密状态,防止中间人攻击。具体而言,数据在发送前由源设备使用对称加密算法(如AES)进行加密,只有目标设备持有解密密钥,确保数据的机密性。同时,结合同态加密算法(如Paillier或BGN),允许在加密数据上进行计算而无需解密,从而保护数据隐私并支持边缘计算节点进行必要的数据处理。其次,数据存储采用区块链技术,将加密数据以区块的形式存储在分布式账本中。每个数据块包含时间戳、加密数据和前一个区块的哈希值,确保数据的不可篡改性和可追溯性。通过智能合约,系统可以自动管理数据的访问权限和验证过程。在访问控制方面,系统根据用户角色(如管理员、普通用户、访客等)分配不同的访问权限,确保只有授权用户才能访问特定数据。同时,结合生物特征(如指纹、面部识别)和行为特征(如用户的操作习惯、登录时间等),提供多种认证方式,增强安全性。用户在访问系统时,需通过多因素认证(MFA)进行身份验证,确保只有合法用户能够访问敏感数据。最后,结合WiFi探针技术,在边缘服务器、边缘计算节点和目标物联网开关设备上实时采集性能指标(如网络延迟、数据传输速率、设备负载等),并通过数据分析工具监控系统性能。这些性能指标将用于优化网络配置和资源分配,确保系统在高负载情况下仍能保持高效运行。

[0047] 通过以上步骤,本实施例能够实现数据的安全保护、访问控制和性能监控,确保物联网环境中的数据安全和设备可靠性。

[0048] 作为一种可选的实施方式,在智能家居环境中,部署本发明的物联网开关控制方法,步骤具体如下:

1、边缘节点部署,在家庭网关处部署边缘计算节点,内置智能控制模块。

- [0049] 2、设备连接,智能灯光、空调等开关设备接入边缘节点。
- [0050] 3、本地数据处理和控制,当传感器检测到有人进入房间时,边缘节点立即控制灯光开启;根据室内温度和预设条件,自动调节空调的开关和温度设置。
- [0051] 4、安全通信,所有数据传输均采用AES加密算法,确保通信安全。
- [0052] 5、云端协同,用户可通过手机App连接云端服务器,远程查看设备状态和控制日志。
- [0053] 作为另一种可选的实施方式,在工业物联网中,应用本发明的方法对生产线设备进行控制,具体步骤如下:
- 1、边缘节点部署,在生产车间部署高性能边缘计算节点。
- [0054] 2、设备连接,车间内的机器设备和传感器连接至边缘节点。
- [0055] 3、本地数据处理和控制,实时监测设备运行状态,如温度、振动等参数。当检测到异常情况时,边缘节点立即发出指令,停止设备运行,防止事故发生。
- [0056] 4、安全通信,利用VPN和SSL协议建立安全通信通道。
- [0057] 5、云端协同,生产数据和设备日志定期上传云端,支持大数据分析和决策。
- [0058] 对应上述方法,本实施例还提供了一种基于边缘计算的物联网开关控制系统,包括:
- 部署模块,用于在目标物联网开关设备的网络边缘部署一个边缘服务器和多个边缘计算节点;
- 连接模块,用于控制目标物联网开关设备通过无线或有线方式与各个边缘节点建立连接,以进行数据交互;
- 数据处理模块,用于利用边缘节点采集所述目标物联网开关设备的状态数据,并对所述状态数据进行数据处理和异常检测,得到数据检测结果;
- 计算模块,用于控制所述边缘服务器采集各个所述边缘计算节点的通信状态数据,并根据所述通信状态数据各个所述边缘计算节点之间的连接关系;
- 控制模块,用于根据所述数据检测结果生成控制指令,并通过所述边缘节点向所述目标物联网开关设备发送所述控制指令,以实现实时控制;
- 保护模块,用于根据所述边缘计算节点的数据处理和异常检测过程,进行所述边缘服务器的实时更新和优化,并进行组网策略的动态调整,并在所述边缘服务器、所述边缘计算节点和所述目标物联网开关设备中引入加密技术和访问控制策略,以进行数据的安全保护。
- [0059] 本发明的有益效果如下:
- (1) 本发明通过在网络边缘部署边缘服务器和计算节点,数据处理和控制指令的生成可以在本地完成,显著降低了数据传输的延迟。这对于需要快速响应的应用场景(如智能家居、工业自动化等)尤为重要。
- [0060] (2) 本发明的边缘节点能够在数据产生的地点进行实时数据处理和异常检测,减少了对云端的依赖,降低了网络带宽的占用,提高了数据处理的效率。
- [0061] (3) 本发明的边缘计算架构可以在网络不稳定或断网的情况下继续工作,确保系统的可靠性和稳定性。即使与云端的连接中断,边缘节点仍能执行本地控制和监测。
- [0062] (4) 本发明通过在边缘节点进行数据处理和过滤,可以仅将重要的、经过处理的数

据上传至云端,减少了数据传输量,从而节省了带宽和相关的成本。

[0063] (6) 本发明在边缘服务器和计算节点中引入加密技术和访问控制策略,能够有效保护数据的安全性,防止数据泄露和未授权访问。这对于物联网设备的安全性至关重要。

[0064] (7) 本发明的边缘服务器能够根据各个边缘计算节点的数据处理和异常检测结果进行实时更新和优化,动态调整网络策略,以适应不断变化的环境和需求。

[0065] (8) 本发明可以广泛应用于智能家居、工业自动化、智慧城市等多个领域,具有良好的灵活性和可扩展性,能够根据不同的应用需求进行调整和优化。

[0066] (9) 本发明通过实时监测和控制,用户能够获得更智能化的体验,例如自动调节灯光、温度等,提升了生活和工作的舒适度。

[0067] (10) 本发明通过对状态数据的实时分析和异常检测,系统能够提供更准确的决策支持,帮助用户及时发现和解决潜在问题。

[0068] 本说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似部分互相参见即可。对于实施例公开的系统而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0069] 本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处。综上所述,本说明书内容不应理解为对本发明的限制。

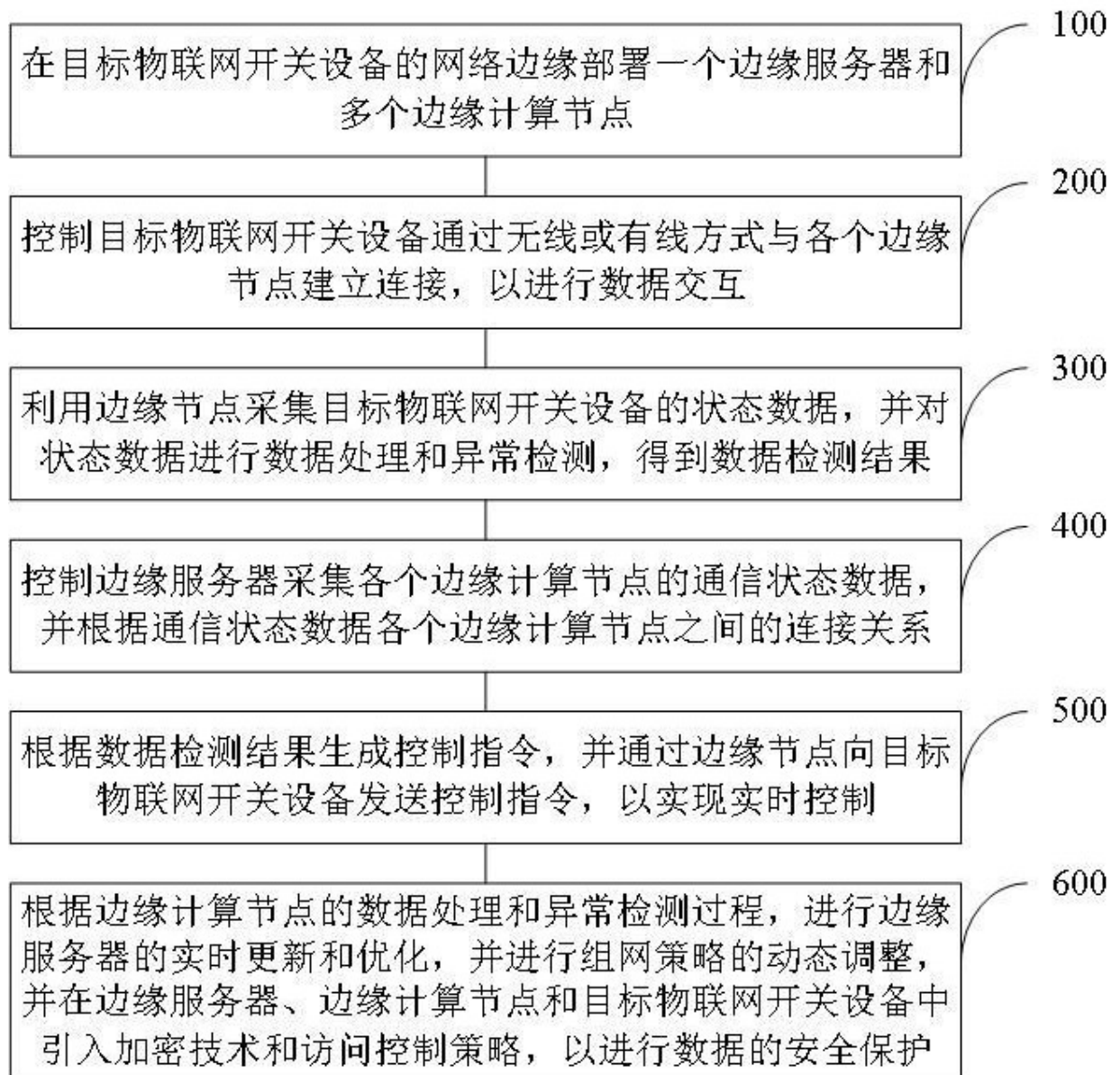


图 1