(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114666210 B
(45)授权公告日 2022.08.16

(21)申请号 202210559546.5

(22)申请日 2022.05.23

(65)同一申请的已公布的文献号
申请公布号 CN 114666210 A

(43)申请公布日 2022.06.24

(73)专利权人 江苏金融租赁股份有限公司
地址 210000 江苏省南京市建邺区嘉陵江东街99号金融城1号楼8-9、11-19、25-33层

(72)发明人 毛克特 王宗力 口拴军 张睿甫 鞠高明 张伶俐

(74)专利代理机构 南京瑞华腾知识产权代理事务所(普通合伙) 32368
专利代理师 李超

(51)Int.Cl.
H04L 41/069(2022.01)
H04L 41/142(2022.01)
G06K 9/62(2022.01)

(56)对比文件
CN 112395156 A,2021.02.23
CN 109240895 A,2019.01.18

审查员 高阳

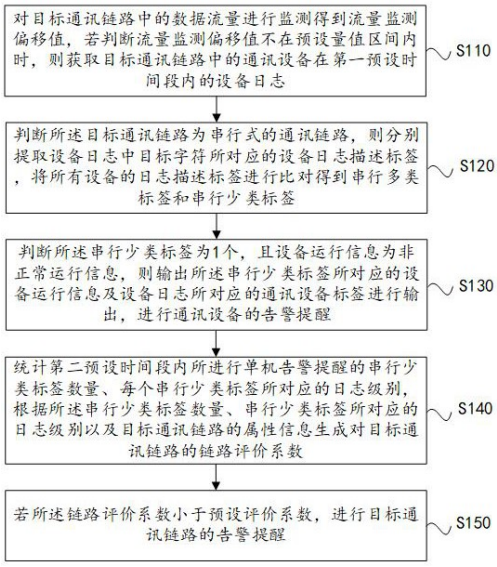
权利要求书4页 说明书14页 附图3页

(54)发明名称

基于大数据日志分析的告警方法及装置

(57)摘要

本发明提供一种基于大数据日志分析的告警方法及装置，包括：获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；判断目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签；判断串行少类标签为1个，且设备运行信息为非正常运行信息，则输出串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签进行输出，进行通讯设备的告警提醒；根据串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数；若链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒。



CN 114666210 B

1.基于大数据日志分析的告警方法,其特征在于,包括:

对目标通讯链路中的数据流量进行监测得到流量监测偏移值,若判断流量监测偏移值不在预设量值区间内时,则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志;

判断所述目标通讯链路为串行式的通讯链路,则分别提取设备日志中目标字符所对应的设备日志描述标签,将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签,所述串行多类标签为相同类型数量多的日志描述标签,所述串行少类标签为相同类型数少的日志描述标签;

判断所述串行少类标签为1个,且设备运行信息为非正常运行信息,则输出所述串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签,进行通讯设备的告警提醒;

统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别,根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数;

若所述链路评价系数小于预设评价系数,进行目标通讯链路的告警提醒;

在对目标通讯链路中的数据流量进行监测得到流量监测偏移值,若判断流量监测偏移值不在预设量值区间内时,则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中,具体包括:

确定目标通讯链路中的数据发送设备、至少一个中继传输设备以及至少一个数据接收设备;

在所述数据发送设备和与其相邻的中继传输设备之间设置发送数据采集点,用于采集数据发送设备所发送的发送数据量值;

在所述数据接收设备和与其相邻的中继传输设备之间设置接收数据采集点,用于采集数据接收设备所接收的接收数据量值;

根据所述发送数据量值和接收数据量值生成流量监测偏移值,若所述流量监测偏移值不在预设量值区间内时,则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志;

在根据所述发送数据量值和接收数据量值生成流量监测偏移值,若所述流量监测偏移值不在预设量值区间内时,则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中,具体包括:

获取目标通讯链路中所有中继设备的数量、每个中继设备的接入终端数量,根据所有中继设备的数量、每个中继设备的接入终端数量生成偏移系数;

根据所述发送数据量值、接收数据量值以及偏移系数生成流量监测偏移值;

通过以下公式计算流量监测偏移值,

$$p_y = k_1 \cdot \frac{x_1 - x_2}{s} \cdot \frac{1}{u^{N \cdot \frac{\sum_{i=1}^{n} l_i}{N}}}$$

其中,p_y为流量监测偏移值,k_1为流量偏移权重,x_1为发送数据量值,x_2为接收数据

量值，s为第一常数值，u为第二常数值，N为中继设备的数量，l_i为第 i 个中继设备的接入终端数量，n 为中继设备的上限值。

2.根据权利要求1所述的基于大数据日志分析的告警方法，其特征在于，还包括：

若判断所有设备的日志描述标签进行比对后为同一个串行多类标签，则判断此时流量监测偏移值的计算过大，获取所述预设量值区间的上边界点和下边界点；

确定与此时流量监测偏移值相对应的上边界点或下边界点，通过以下公式对流量偏移权重k_1进行缩小处理，

$$\begin{cases} 若p_y > b_1，\ 则k_2 = k_1 - k_1 \cdot \dfrac{p_y - b_1}{h_1} \\ 若p_y < b_2，\ 则k_2 = k_1 - k_1 \cdot \dfrac{b_2 - p_y}{h_2} \end{cases}$$

其中，k_2为缩小处理后的流量偏移权重，b_1为预设量值区间的上边界点，b_2为预设量值区间的下边界点，h_1为第一调整系数，h_2为第二调整系数。

3.根据权利要求1所述的基于大数据日志分析的告警方法，其特征在于，

在判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签的步骤中，具体包括：

获取目标通讯链路所对应的模式标签，若所述模式标签为串行式则判断所述目标通讯链路为串行式的通讯链路，所述模式标签为管理员预先设置；

提取目标字符所对应的设备日志描述标签，每种通讯设备运行内容具有与其对应的设备日志描述标签；

对所有通讯设备的设备日志描述标签进行归类统计，得到每种日志描述标签的数量；

若判断日志描述标签共存在2类，则对每种日志描述标签的数量进行比对，将数量较多的日志描述标签作为串行多类标签，将数量较少的日志描述标签作为串行少类标签。

4.根据权利要求1所述的基于大数据日志分析的告警方法，其特征在于，

在判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则输出所述串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签，进行通讯设备的告警提醒的步骤中，具体包括：

将串行少类标签与预设的非正常运行标签比对，若串行少类标签与非正常运行标签中的任意一个相对应，则判断与串行少类标签对应的设备运行信息为非正常运行信息；

获取串行少类标签所对应的设备日志的通讯设备标签，将所述通讯设备标签、设备运行信息以及提醒信号输出。

5.根据权利要求4所述的基于大数据日志分析的告警方法，其特征在于，

在统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数的步骤中，具体包括：

提取数据库中在第一预设时间段内预先存储的告警提醒的串行少类标签数量、以及每个串行少类标签所对应的日志级别，对每个串行少类标签所对应的日志级别按照危害程度呈反比的量化处理；

对目标通讯链路的属性信息进行量化处理；

根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数。

6.根据权利要求5所述的基于大数据日志分析的告警方法，其特征在于，

在根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数的步骤中，具体包括：

通过以下公式计算目标通讯链路的链路评价系数，

$$c=\frac{\sum_{\alpha}^{\beta}d_{\alpha}}{j}\cdot\frac{1}{a^{j}}\cdot\frac{1}{b^{r}}\cdot\gamma$$

其中，c为目标通讯链路的链路评价系数，d_{α}为第α个串行少类标签所对应的量化后的日志级别，β为串行少类标签的上限值，j为串行少类标签的数量值，a为第三常数值，b为通讯链路量化后的属性信息，r为第四常数值，γ为链路评价系数权重值。

7.根据权利要求6所述的基于大数据日志分析的告警方法，其特征在于，

在若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒的步骤后，具体包括：

获取第三时间段内的管理员的行为数据；

若所述行为数据为对目标通讯链路中的至少一个通讯设备进行调整，则对计算目标通讯链路中的预设评价系数进行减小调整；

若所述行为数据为对目标通讯链路中的所有通讯设备不进行调整，则对计算目标通讯链路中的预设评价系数进行增加调整。

8.基于大数据日志分析的告警装置，其特征在于，包括：

监测模块，用于对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；

比对模块，用于判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签，所述串行多类标签为相同类型数量多的日志描述标签，所述串行少类标签为相同类型数少的日志描述标签；

设备告警模块，用于判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则输出所述串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签，进行通讯设备的告警提醒；

链路评价模块，用于统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数；

链路告警模块，用于若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒；

在对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中，具体包括：

确定目标通讯链路中的数据发送设备、至少一个中继传输设备以及至少一个数据接收设备；

在所述数据发送设备和与其相邻的中继传输设备之间设置发送数据采集点，用于采集数据发送设备所发送的发送数据量值；

在所述数据接收设备和与其相邻的中继传输设备之间设置接收数据采集点，用于采集数据接收设备所接收的接收数据量值；

根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；

在根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中，具体包括：

获取目标通讯链路中所有中继设备的数量、每个中继设备的接入终端数量，根据所有中继设备的数量、每个中继设备的接入终端数量生成偏移系数；

根据所述发送数据量值、接收数据量值以及偏移系数生成流量监测偏移值；

通过以下公式计算流量监测偏移值，

$$p_y = k_1 \cdot \frac{x_1 - x_2}{s} \cdot \frac{1}{u^N \cdot \frac{\sum_{i=1}^{n} l_i}{N}}$$

其中，p_y为流量监测偏移值，k_1为流量偏移权重，x_1为发送数据量值，x_2为接收数据量值，s为第一常数值，u为第二常数值，N为中继设备的数量，l_i为第 i 个中继设备的接入终端数量，n为中继设备的上限值。

基于大数据日志分析的告警方法及装置

技术领域

[0001] 本发明涉及大数据技术领域，尤其涉及一种基于大数据日志分析的告警方法及装置。

背景技术

[0002] 在大数据技术领域里，数据来源有很多：关系型数据库、爬虫、日志等等。日志用于记录程序运行时的信息，生产环境需要记录的日志较多，在得到日志后，会对日志进行存储。

[0003] 通过日志可以反映出设备的工作状态。对于通讯领域来来说，一个通讯链路可能会包括多个用于数据传输的传输设备，通讯链路具有多种，例如串行的通讯链路、并行的通讯链路等等。串行的通讯链路可以理解为只有一个数据传输支路，在串行的通讯链路中任意一个传输设备出现问题时，则此时可能会导致整个通讯链路无法正常传输，此时用户只是知道数据出现无法正常传输的情况，但是并不知道存在何种原因、某个设备的情况导致无法正常传输，无法确定相应的原因而进行告警；

[0004] 所以亟需一种技术方案，能够在串行的通讯链路的场景下，在出现数据传输异常时，进行自动的、快速的定位到出现问题的传输设备。

发明内容

[0005] 本发明实施例提供一种基于大数据日志分析的告警方法及装置，可以在串行的通讯链路的场景下，通过日志分析快速定位到出现问题的传输设备，并且能够对该目标通讯链路的在一定时间段内的使用情况进行分析，保障系统、通讯链路的高可用性。

[0006] 本发明实施例的第一方面，提供一种基于大数据日志分析的告警方法，包括：

[0007] 对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；

[0008] 判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签，所述串行多类标签为相同类型数量多的日志描述标签，所述串行少类标签为相同类型数少的日志描述标签；

[0009] 判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则对所述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，进行通讯设备的告警提醒；

[0010] 统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数；

[0011] 若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒。

[0012] 可选地，在第一方面的一种可能实现方式中，在对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中，具体包括：

[0013] 确定目标通讯链路中的数据发送设备、至少一个中继传输设备以及至少一个数据接收设备；

[0014] 在所述数据发送设备和与其相邻的中继传输设备之间设置发送数据采集点，用于采集数据发送设备所发送的发送数据量值；

[0015] 在所述数据接收设备和与其相邻的中继传输设备之间设置接收数据采集点，用于采集数据接收设备所接收的接收数据量值；

[0016] 根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志。

[0017] 可选地，在第一方面的一种可能实现方式中，在根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志的步骤中，具体包括：

[0018] 获取目标通讯链路中所有中继设备的数量、每个中继设备的接入终端数量，根据所有中继设备的数量、每个中继设备的接入终端数量生成偏移系数；

[0019] 根据所述发送数据量值、接收数据量值以及偏移系数生成流量监测偏移值；

[0020] 通过以下公式计算流量监测偏移值，

[0021] $$p_y = k_1 \cdot \frac{x_1 - x_2}{s} \cdot \frac{1}{u^N \cdot \frac{\sum_{i=1}^{n} l_i}{N}}$$

[0022] 其中，p_y为流量监测偏移值，k_1为流量偏移权重，x_1为发送数据量值，x_2为接收数据量值，s为第一常数值，u为第二常数值，N为中继设备的数量，l_i为第i个中继设备的接入终端数量，n为中继设备的上限值。

[0023] 可选地，在第一方面的一种可能实现方式中，还包括：

[0024] 若判断所有设备的日志描述标签进行比对后为同一个串行多类标签，则判断此时流量监测偏移值的计算过大，获取所述预设量值区间的上边界点和下边界点；

[0025] 确定与此时流量监测偏移值相对应的上边界点或下边界点，通过以下公式对流量偏移权重k_1进行缩小处理，

[0026] $$\begin{cases} p_y > b_1, \ k_2 = k_1 - k_1 \cdot \frac{p_y - b_1}{h_1} \\ p_y < b_2, \ k_2 = k_1 - k_1 \cdot \frac{b_2 - p_y}{h_2} \end{cases}$$

[0027] 其中，k_2为缩小处理后的流量偏移权重，b_1为预设量值区间的上边界点，b_2为预设量值区间的下边界点，h_1为第一调整系数，h_2为第二调整系数。

[0028] 可选地，在第一方面的一种可能实现方式中，在判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签的步骤中，具体包括：

[0029] 获取目标通讯链路所对应的模式标签，若所述模式标签为串行式则判断所述目标通讯链路为串行式的通讯链路，所述模式标签为管理员预先设置；

[0030] 提取目标字符所对应的设备的日志描述标签，每种通讯设备运行内容具有与其对应的设备的日志描述标签；

[0031] 对所有设备的日志描述标签进行归类统计，得到每种日志描述标签的数量；

[0032] 若判断日志描述标签共存在2类，则对每种日志描述标签的数量进行比对，将数量较多的日志描述标签作为串行多类标签，将数量较少的日志描述标签作为串行少类标签。

[0033] 可选地，在第一方面的一种可能实现方式中，在判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则对所述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，进行通讯设备的告警提醒的步骤中，具体包括：

[0034] 将串行少类标签与预设的非正常运行标签比对，若串行少类标签与非正常运行标签中的任意一个相对应，则判断与串行少类标签对应的设备运行信息为非正常运行信息；

[0035] 获取串行少类标签所对应的设备日志的通讯设备标签，将所述通讯设备标签、设备运行信息以及提醒信号输出。

[0036] 可选地，在第一方面的一种可能实现方式中，在统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数的步骤中，具体包括：

[0037] 提取数据库中在第一预设时间段内预先存储的告警提醒的串行少类标签数量、以及每个串行少类标签所对应的日志级别，对每个串行少类标签所对应的日志级别按照危害程度呈反比的量化处理；

[0038] 对目标通讯链路的属性信息进行量化处理；

[0039] 根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数。

[0040] 可选地，在第一方面的一种可能实现方式中，在根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数的步骤中，具体包括：

[0041] 通过以下公式计算目标通讯链路的链路评价系数，

[0042] $$c=\frac{\sum_{\alpha}^{\beta}d_{\alpha}}{j}\cdot\frac{1}{a^{j}}\cdot\frac{1}{b^{r}}\cdot\gamma$$

[0043] 其中，c为目标通讯链路的链路评价系数，d_{α}为第α个串行少类标签所对应的量

化后的日志级别，β为串行少类标签的上限值，j为串行少类标签的数量值，a为第三常数值，b为通讯链路量化后的属性信息，r为第四常数值，γ为链路评价系数权重值。

[0044] 可选地，在第一方面的一种可能实现方式中，在若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒的步骤后，具体包括：

[0045] 获取第三时间段内的管理员的行为数据；

[0046] 若所述行为数据为对目标通讯链路中的至少一个通讯设备进行调整，则对计算目标通讯链路中的预设评价系数进行减小调整；

[0047] 若所述行为数据为对目标通讯链路中的所有通讯设备不进行调整，则对计算目标通讯链路中的预设评价系数进行增加调整。

[0048] 本发明实施例的第二方面，提供一种基于大数据日志分析的告警装置，包括：

[0049] 监测模块，用于对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；

[0050] 比对模块，用于判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签；

[0051] 设备告警模块，用于判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则对所述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，进行通讯设备的告警提醒；

[0052] 链路评价模块，用于统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数；

[0053] 链路告警模块，用于若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒。

[0054] 本发明实施例的第三方面，提供一种存储介质，所述存储介质中存储有计算机程序，所述计算机程序被处理器执行时用于实现本发明第一方面及第一方面各种可能设计的所述方法。

[0055] 本发明提供的一种基于大数据日志分析的告警方法及装置。能够对串行式的通讯链路中的通讯状态进行监测，在可能会出现数据传输的数据量、流量出现问题时，则主动获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志，然后对第一预设时间段内的设备日志进行整体的信息提取、进行日志的标签归类，根据日志描述标签的比对结果快速确定出现问题的通讯设备，并针对该通讯设备输出相应的告警提醒。本发明在针对某个通讯设备输出相应的告警提醒后，还会对整个目标通讯链路在第二预设时间段内各个通讯设备的整体情况进行统计，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数，通过链路评价系数来反应出目标通讯链路的在未来时间段的使用情况，进而输出相应的告警提醒，以使管理员对目标通讯链路进行整体的、预防性的维护。

[0056] 本发明提供的技术方案，会对数据发送设备和数据接收设备之间的数据流量进行统计，并根据数据发送设备和数据接收设备处的数据流量的关系得到相对应的流量监测偏移值，在进行流量监测偏移值的计算时，本发明会综合考虑每个目标通讯链路处中继设备的数量、中继设备的接入终端数量等维度的信息，使得每个目标通讯链路都会具有与其相对应的流量监测偏移值，使得所得到的流量监测偏移值更适宜当前的监测、计算场景。

[0057] 本发明提供的技术方案，在判断所有设备的日志描述标签进行比对后为同一个串行多类标签，则证明此时所有通讯设备都处于相同的工作状态，此时所计算的流量监测偏移值是虚大的，所以此时需要对相同场景下所计算的流量监测偏移值进行减小处理。所以此时，本发明会采取主动学习的方式，根据流量监测偏移值、相对应的上边界点或下边界点对流量偏移权重进行缩小处理，流量偏移权重所缩小处理的幅度与流量监测偏移值的数量大小存在关联性，进而达到对计算流量监测偏移值的公式持续更新、训练的目的。

附图说明

[0058] 图1为本发明中所说的串行式的通讯链路的结构示意图；

[0059] 图2为基于大数据日志分析的告警方法的第一种实施方式的流程图；

[0060] 图3为基于大数据日志分析的告警方法的第二种实施方式的流程图；

[0061] 图4为基于大数据日志分析的告警装置的第一种实施方式的结构图。

具体实施方式

[0062] 为使本发明实施例的目的、技术方案和优点更加清楚，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。

[0063] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等(如果存在)是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。

[0064] 应当理解，在本发明的各种实施例中，各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0065] 应当理解，在本发明中，“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0066] 应当理解，在本发明中，“多个”是指两个或两个以上。“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。“包含A、B和C”、“包含A、B、C”是指A、B、C三者都包含，“包含A、B或C”是指包含A、B、C三者之一，“包含A、B和/或C”是指包含A、B、C三者中任1个或任2个或3个。

[0067] 应当理解，在本发明中，“与A对应的B”、“与A相对应的B”、“A与B相对应”或者“B与A相对应”，表示B与A相关联，根据A可以确定B。根据A确定B并不意味着仅仅根据A确定B，还可以根据A和/或其他信息确定B。A与B的匹配，是A与B的相似度大于或等于预设的阈值。

[0068] 取决于语境，如在此所使用的“若”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。

[0069] 下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0070] 如图1所示，为本发明提供的技术方案所适用的数据传输场景，可以理解为是本发明中所说的串行式的通讯链路，可以包括数据发送设备、数据接收设备以及多个中继设备，数据发送设备通过多个中继设备发送至数据接收设备。中继设备可以是路由器、网关、交换机等等。数据发送设备、数据接收设备以及多个中继设备所构成的数据传输路径可以是本发明所说的串行式的通讯链路，任意两个相邻的设备之间的数据传输路径、链路可以是一个子链路。

[0071] 本发明提供一种基于大数据日志分析的告警方法，如图2所示，包括：

[0072] 步骤S110、对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志。本发明提供的技术方案，会根据数据流量来判断目标通讯链路是否正常工作，一般来说，某个通讯设备出现异常时，可能会出现直接停止数据传输、大幅减少数据传输的情况。在目标通讯链路中，任意一个中继设备出现异常，都会造成流量监测偏移值较大的情况，流量监测偏移值可以认为是同一个目标通讯链路中不同子通讯链路的数据传输量值的差值、偏移值。在判断流量监测偏移值不在预设量值区间内时，则证明此时目标通讯链路中很可能出现了通讯设备不能工作、无法正常工作的情况，所以此时需要获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志，根据设备日志来对目标通讯链路中所有通讯设备进行快速的诊断，确定存在问题的通讯设备。

[0073] 本发明提供的技术方案，在一个可能的实施方式中，如图3所示，步骤S110具体包括：

[0074] 步骤S1101、确定目标通讯链路中的数据发送设备、至少一个中继传输设备以及至少一个数据接收设备。本发明提供的技术方案，首先会根据目标通讯链路中不同通讯设备的作用将通讯设备分为数据发送设备、中继传输设备以及数据接收设备，数据发送设备例如说是摄像头、拾音器、移动终端等等，中继传输设备例如说路由器、网关、交换机等等，数据接收设备例如说是显示端、服务器等等。不同通讯目的的目标通讯链路会具有不同的数据发送设备、中继传输设备以及数据接收设备。

[0075] 步骤S1102、在所述数据发送设备和与其相邻的中继传输设备之间设置发送数据采集点，用于采集数据发送设备所发送的发送数据量值。本发明提供的技术方案，会通过发送数据采集点采集数据发送设备所发送的数据量值，例如数据发送设备是摄像头，其对视频数据打包后会进行发送，本发明中的发送数据采集点即可以对摄像头所发送的视频数据进行监测得到发送数据量值。在一个可能的实施方式中，发送数据采集点可以是在数据发送设备处设置的发送信息采集模块，通过发送信息采集模块能够对所发送的、打包后的视频数据的发送数据量值进行发送。

[0076] 步骤S1103、在所述数据接收设备和与其相邻的中继传输设备之间设置接收数据采集点，用于采集数据接收设备所接收的接收数据量值。本发明提供的技术方案，会通过接收数据采集点采集数据接收设备所接收的数据量值，例如数据接收设备是移动终端，其会接收各个中继设备所传输的、打包后的视频数据，本发明中的接收数据采集点即可以对中继设备所发送的视频数据进行监测得到接收数据量值。在一个可能的实施方式中，接收数据采集点可以是在数据接收设备处设置的接收信息采集模块，通过接收信息采集模块能够对所接收的、打包后的视频数据的接收数据量值进行存储。

[0077] 步骤S1104、根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志。一般来说，在信息、数据的发送、传输过程中，经过多方的传输，可能会出现部分数据遗失、减少的情况，也可能会出现视频数据在各个中继设备传输、解析、加密的过程造成数据量值增加的情况。所以，本发明会根据发送数据量值和接收数据量值生成流量监测偏移值，该流量监测偏移值可能是正值、也可能是负值，如果流量监测偏移值不在预设量值区间内，则证明此时数据遗失量过多，或数据增加量过多，甚至是发送数据量值正常，但接收数据量值很小的情况。

[0078] 在流量监测偏移值不在预设量值区间内时，则此时可能会出现一个设备存在问题，所以本发明提供的技术方案会得到标通讯链路中的通讯设备在第一预设时间段内的设备日志。

[0079] 通讯设备出现问题例如说是电源不稳定、冷启动、CPU处理量较大无法进行正常的数据传输、出现BUG、设备过热需要降低运算量等等，对于设备出现问题的形式本发明不做任何限定。

[0080] 本发明提供的技术方案，在一个可能的实施方式中，步骤S1104具体包括：

[0081] 获取目标通讯链路中所有中继设备的数量、每个中继设备的接入终端数量，根据所有中继设备的数量、每个中继设备的接入终端数量生成偏移系数。一般来说，目标通讯链路中所有中继设备的数量越大，则产生丢包、数据丢失的情况几率越大，中继设备的接入终端数量越多，则该中继设备产生的错误可能就越大。同样的，中继设备的数量、每个中继设备的接入终端数量越多，则对于一个视频数据中所额外加载信息可能就越大。以上所说的数据量的丢失、额外加载信息的添加都是属于正常的通信场景，所以本发明会根据接入终端数量，根据所有中继设备的数量、每个中继设备的接入终端数量生成偏移系数。

[0082] 根据所述发送数据量值、接收数据量值以及偏移系数生成流量监测偏移值。本发明提供的技术方案，会根据发送数据量值、接收数据量值得到所发送的数据和所接收的数据的差值，如果发送数据量值和接收数据量值的差值的绝对值较大，则证明此时可能会存在丢失数据较多、添加信息较多的异常情况。在极端的场景下，例如说某个中继设备产生出现了损害的情况(冷启动)，则在某个时间段时，中继设备无法进行正常的数据传输，此时数据发送端发送的视频数据的发送数据量值和接收数据量值的差值就会较大。

[0083] 通过以下公式计算流量监测偏移值，

[0084] $$p_y = k_1 \cdot \frac{x_1 - x_2}{s} \cdot \frac{1}{u^N \cdot \frac{\sum_{i=1}^{n} l_i}{N}}$$

[0085] 其中，p_y为流量监测偏移值，k_1为流量偏移权重，x_1为发送数据量值，x_2为接收数据量值，s为第一常数值，u为第二常数值，N为中继设备的数量，l_i为第i个中继设备的接入终端数量，n为中继设备的上限值。

[0086] 通过$\frac{x_1 - x_2}{s}$可以得到发送数据量值和接收数据量值的差值，通过$u^N \cdot \frac{\sum_{i=1}^{n} l_i}{N}$可以得到偏移系数，如果所有中继设备的数量、每个中继设备的接入终端数量越大，则此时可能会造成发送数据量值和接收数据量值的差值就会较大，此时需要一个较小的偏移系数，通过偏移系数对$\frac{x_1 - x_2}{s}$进行修正，所以流量监测偏移值是与偏移系数呈反向趋势的。流量监测偏移值越大，则证明在相应的场景下，发送数据量值和接收数据量值的差值、差距就会较大。通过$\frac{\sum_{i=1}^{n} l_i}{N}$可以得到每一个中继设备平均所连接的接入终端数量。

[0087] 步骤S120、判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签，所述串行多类标签为相同类型数量多的日志描述标签，所述串行少类标签为相同类型数少的日志描述标签。一般来说，本发明提供的技术方案适用于目标通讯链路为串行式的通讯链路中，即数据、信息的传输都是点对点的，但是可以一个数据发送设备对应多个数据接收设备，即一个数据发送设备分别向多个数据接收设备发送数据，也可以是多个数据发送设备分别向一个数据接收设备发送数据，在正常的数据传输过程中，数据发送和数据接收的数据量值是一定的、相对应的。

[0088] 以中继设备为交换机为例，其可以设备日志可以如下：

[0089] Jul15202119:37:30+08:00CORESNMP/4/COLDSTART:OID1.3.6.1.6.3.1.1.5.1 coldStart。

[0090] Jul15202119:37:30+08:00可以是时间戳，理解为是日志产生的时间，本发明会选取时间戳在第一预设时间段内的设备日志。

[0091] CORE，意思是主机名，表示设备的名称，其默认名称是HUAWEI、Xiaomi等等。

[0092] 4，日志级别，可以共有八级，例如0-7，一般来说数字越小，日志越严重，即通讯设备的故障越严重。

[0093] SNMP，模块名，表示日志是从哪个模块产生的，通讯设备可以根据管理员的需要预先配置多个模块。

[0094] COLDSTART为信息摘要，日志的概括信息，即可理解为设备的日志描述标签，设备日志中目标字符即可以是COLDSTART。

[0095] OID 1.3.6.1.6.3.1.1.5.1 ,mib节点,SNMP的mib节点信息,与本发明提供的技术方案不相关联,所以不再进行说明。

[0096] coldStart为详细信息,用于详细描述日志的具体内容,与信息摘要相对应。

[0097] 以上的交换机可以是华为交换机S7706的日志。

[0098] 本发明提供的技术方案,在一个可能的实施方式中,步骤S120具体包括:

[0099] 获取目标通讯链路所对应的模式标签,若所述模式标签为串行式则判断所述目标通讯链路为串行式的通讯链路,所述模式标签为管理员预先设置。一般来说,管理员可以根据不同目标通讯链路的情况为其主动设置模式标签。模式标签可以是串行式、并行式等等,本发明中只是针对串行式的目标通讯链路进行故障的通讯设备的快速定位。本发明提供的技术方案,会首先确定目标通讯链路为串行式的通讯链路。

[0100] 提取目标字符所对应的设备的日志描述标签,每种通讯设备运行内容具有与其对应的设备的日志描述标签。一般来说,本发明会首先确定每一个设备日志的目标字符,不同设备、不同厂家的目标字符可以是不同的,例如华为的交换机的目标字符即可能是COLDSTART,小米的路由器的目标字符即可能是其他字母。本发明会提取每个通讯设备所对应的目标字符的日志描述标签。

[0101] 日志描述标签可以是本发明预先为每个通讯设备预先配置的,例如说在某个设备出现冷启动时,则此时日志描述标签具有冷启动字符,例如说某个设备过热而进行自我保护时,则此时日志描述标签具有自我保护字符,例如说在某个设备进行正常数据传输时,则此时日志描述标签具有数据正常传输字符。

[0102] 对所有设备的日志描述标签进行归类统计,得到每种日志描述标签的数量。本发明会对所有设备的日志描述标签进行归类统计,例如一共存在4个中继设备,1个中继设备为冷启动字符,另外3个设备为正常数据传输字符,则此时日志描述标签所对应的冷启动字符的数量即为1、日志描述标签所对应的正常数据传输字符的数量即为3。

[0103] 对于日志描述标签所包括的冷启动字符、正常数据传输字符等可以简化替代,例如L1、L2等等。

[0104] 若判断日志描述标签共存在2类,则对每种日志描述标签的数量进行比对,将数量较多的日志描述标签作为串行多类标签,将数量较少的日志描述标签作为串行少类标签。在日志描述标签为2种类型时,此时本发明会将根据每种日志描述标签的数量对日志描述标签进行分类,得到串行多类标签和串行少类标签。例如冷启动字符的数量为1、正常数据传输字符的数量为3,则此时串行多类标签对应为正常数据传输字符,串行少类标签对应为冷启动字符。

[0105] 一般来说,目标通讯链路中的某个通讯设备出现故障时,只会存在少量的通讯设备出现问题,所以此时大多数的通讯设备都是正常的,所以此时会存在2种类型的日志描述标签,并且数量少的日志描述标签较大概率是故障通讯设备所对应的日志描述标签。所以,本发明会根据每种类型的日志描述标签的数量对日志描述标签进行归类,得到串行多类标签以及串行少类标签。

[0106] 本发明提供的技术方案,在一个可能的实施方式中,还包括:

[0107] 若判断所有设备的日志描述标签进行比对后为同一个串行多类标签,则判断此时流量监测偏移值的计算过大,获取所述预设量值区间的上边界点和下边界点。如果所有设

备的日志描述标签进行比对后为同一个串行多类标签，则此时大概率所有设备的日志描述标签都是正常数据传输字符，即此时可能所计算的流量监测偏移值出现与实际场景不适配的情况，即认为此时流量监测偏移值的计算过大。所以本发明会选取预设量值区间的上边界点和下边界点。预设量值区间可以是$[b_2,\ b_1]$，b_1是正值，b_2是负值。

[0108] 确定与此时流量监测偏移值相对应的上边界点或下边界点，通过以下公式对流量偏移权重k_1进行缩小处理，

[0109] $$\begin{cases} p_y > b_1,\ k_2 = k_1 - k_1 \cdot \dfrac{p_y - b_1}{h_1} \\ p_y < b_2,\ k_2 = k_1 - k_1 \cdot \dfrac{b_2 - p_y}{h_2} \end{cases}$$

[0110] 其中，k_2为缩小处理后的流量偏移权重，b_1为预设量值区间的上边界点，b_2为预设量值区间的下边界点，h_1为第一调整系数，h_2为第二调整系数。

[0111] 本发明提供的技术方案，在进行流量监测偏移值的计算时，可能会出现大于0或小于0的情况，例如发送数据量值大于接收数据量值，则此时流量监测偏移值是正值，发送数据量值小于接收数据量值，则此时流量监测偏移值是负值，无论正值还是负值，都会具有一个正常的变动区间，该变动区间即为预设量值区间，预设量值区间可以是管路员根据实际的数据传输场景、目标通讯链路设置的。

[0112] 本发明会根据$\frac{p_y-b_1}{h_1}$得到流量监测偏移值与预设量值区间的上边界点之间的差值，$\frac{p_y-b_1}{h_1}$越大，则此时需要对流量偏移权重调整的幅度就越大，此时需要将流量偏移权重k_1调整的更小。同理，本发明会根据$\frac{b_2-p_y}{h_2}$得到流量监测偏移值与预设量值区间的下边界点之间的差值，$\frac{b_2-p_y}{h_2}$越大，则此时需要对流量偏移权重调整的幅度就越大，此时需要将流量偏移权重k_1调整的更小。通过以上的方式，可以持续对流量偏移权重进行持续的更新，使得所计算的流量监测偏移值越来越准确。

[0113] 步骤S130、判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则对所述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，进行通讯设备的告警提醒。在串行少类标签为1个时，则证明该目标通讯链路中存在一个故障的通讯设备，此时本发明会进一步的验证，判断设备运行信息为非正常运行信息时，则对所

述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，通讯设备标签可以是CORE所对应的信息，在具有多个相同厂家的相同设备时，此时可以对相同厂家的相同设备的CORE进行区分，即CORE1、CORE2等等，使得目标通讯链路中的每个通讯设备标签都是唯一的。此时本发明会认为串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签进行输出，该设备运行信息可以是coldStart，详细描述日志的具体内容，与信息摘要相对应。

[0114] 本发明提供的技术方案，在一个可能的实施方式中，步骤S130具体包括：

[0115] 将串行少类标签与预设的非正常运行标签比对，若串行少类标签与非正常运行标签中的任意一个相对应，则判断与串行少类标签对应的设备运行信息为非正常运行信息。本发明提供的技术方案，会预先设置多个非正常运行标签，非正常运行标签例如所说的冷启动字符、自我保护字符等等。如果串行少类标签与非正常运行标签中的任意一个相对应，则此时串行少类标签对应的设备运行信息为非正常运行信息，可以是冷启动字符、自我保护字符等等。

[0116] 获取串行少类标签所对应的设备日志的通讯设备标签，将所述通讯设备标签、设备运行信息以及提醒信号输出。本发明提供的技术方案，会将通讯设备标签、设备运行信息以及提醒信号输出以对管理员进行提醒，进行通讯设备的定位。使得管理员可以快速确定存在问题的通讯设备以及该通讯设备出现故障时的原因。

[0117] 步骤S140、统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数。本发明提供的技术方案，会统计第二预设时间段内所进行告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，第二预设时间段内的时间长度会大于第一预设时间段的长度，第一预设时间段可以是1小时、第二预设时间段可以是10天、1月等等。

[0118] 本发明提供的技术方案，会统计第二预设时间段内所进行告警提醒的串行少类标签数量，告警提醒的串行少类标签数量越多，则证明目标通讯链路内通讯设备所告警的频率越高。本发明会对串行少类标签所对应的日志级别进行统计，例如冷启动是4，自我保护是6等等，日志级别越小，则越严重。本发明还会确定目标通讯链路的属性信息，例如说某些目标通讯链路所传输的数据较为敏感、重要，所以属性信息就较为重要。同理，例如某些目标通讯链路所传输的数据较为不重要，相应的属性信息就较为不重要。

[0119] 本发明提供的技术方案，在一个可能的实施方式中，步骤S140具体包括：

[0120] 提取数据库中在第一预设时间段内预先存储的告警提醒的串行少类标签数量、以及每个串行少类标签所对应的日志级别，对每个串行少类标签所对应的日志级别按照危害程度呈反比的量化处理。本发明提供的技术方案，会对日志级别按照危害程度呈反比的量化处理，如上所说，冷启动是4，自我保护是6，量化处理的对应关系可以是管理员预先设置、配置的。

[0121] 对目标通讯链路的属性信息进行量化处理。本发明提供的技术方案，会对目标通讯链路的属性信息进行量化处理，例如说属性信息为重要，则量化处理后的属性信息可以是10、属性信息为不重要，则量化处理后的属性信息可以是5。

[0122] 根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每

个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数。本发明提供的技术方案，在对多个维度的信息进行量化处理后，会生成与该目标通讯链路相对应的链路评价系数。

[0123] 本发明提供的技术方案，在一个可能的实施方式中，在根据所述串行少类标签数量、每个串行少类标签所对应的量化后的日志级别、每个通讯链路量化后的属性信息生成对目标通讯链路的链路评价系数的步骤中，具体包括：

[0124] 通过以下公式计算目标通讯链路的链路评价系数，

[0125] $$c=\frac{\sum_{\alpha}^{\beta}d_{\alpha}}{j}\cdot\frac{1}{a^{j}}\cdot\frac{1}{b^{r}}\cdot\gamma$$

[0126] 其中，c为目标通讯链路的链路评价系数，d_{α}为第α个串行少类标签所对应的量化后的日志级别，β为串行少类标签的上限值，为串行少类标签的数量值，a为第三常数值，b为通讯链路量化后的属性信息，r为第四常数值，γ为链路评价系数权重值。

[0127] 通过$\frac{\sum_{\alpha}^{\beta}d_{\alpha}}{j}$可以得到所有串行少类标签所对应的量化后的、平均的日志级别，在串行少类标签的数量值越大时，$\frac{1}{a^{j}}$越小，通讯链路量化后的属性信息越大时，$\frac{1}{b^{r}}$越小，链路评价系数权重值可以是预先设置的。通过链路评价系数可以反应出目标通讯链路在第二预设时间段内的稳定性，链路评价系数越大，则目标通讯链路越不稳定。

[0128] 步骤S150、若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒。如果链路评价系数小于预设评价系数，则证明此时相应的目标通讯链路较为不稳定，所以此时需要输出目标通讯链路的告警提醒，以对管理员进行提醒，使管理员进行相应的维护，保障目标通讯链路的高可用性。

[0129] 本发明提供的技术方案，在一个可能的实施方式中，在若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒的步骤后，具体包括：

[0130] 获取第三时间段内的管理员的行为数据。一般来说，在输出目标通讯链路的告警提醒后，则是告知管理员该目标通讯链路存在一定的不稳定性，需要进行部分目标设备的维修、更换等等。第三时间段可以是未来的一段时间看，可以是10天、20天等等。第三时间段内管路员可能会进行维修，也可能不会进行维修。

[0131] 若所述行为数据为对目标通讯链路中的至少一个通讯设备进行调整，则对计算目标通讯链路中的预设评价系数进行减小调整。如果行为数据为对目标通讯链路中的至少一个通讯设备进行调整，则证明管理员按照本发明所提出的告警提醒对目标通讯链路进行了相应的维护、调整动作，此时可以对计算目标通讯链路中的预设评价系数进行减小调整，该种方式能够调小触发告警提醒的阈值，使得本发明能够持续对目标通讯链路的要求持续提高，以满足用户的需求。

[0132] 其中，对计算目标通讯链路中的预设评价系数进行减小调整的方式可以是按照如

下公式调整，

[0133] $$z_2 = z_1 - \varphi_1 \cdot \omega_1$$

[0134] 其中，z_2为减小调整后的预设评价系数，z_1为减小调整前的预设评价系数，φ_1为减小倍数，ω_1为减小常数值。

[0135] 其中减小倍数φ_1、减小常数值ω_1可以是预先设置的。

[0136] 通过以上的技术方案，使得本发明可以对预设评价系数进行持续的减小调整，以满足用户对目标通讯链路的高可用性的持续要求，使所得到的预设评价系数更适用于当前的计算场景。

[0137] 若所述行为数据为对目标通讯链路中的所有通讯设备不进行调整，则对计算目标通讯链路中的预设评价系数进行增加调整。如果行为数据为不对目标通讯链路中的至少一个通讯设备进行调整，则证明管理员并没有按照本发明所提出的告警提醒对目标通讯链路进行相应的维护、调整动作，此时可以对计算目标通讯链路中的预设评价系数进行增加调整，该种方式能够增大触发告警提醒的阈值，使得本发明能够持续对目标通讯链路的要求持续降低，以满足用户的需求。

[0138] 其中，对计算目标通讯链路中的预设评价系数进行增加调整的方式可以是按照如下公式调整，

[0139] $$z_2 = z_1 + \varphi_2 \cdot \omega_2$$

[0140] 其中，φ_2为增加倍数，ω_2为增加常数值。

[0141] 其中增加倍数φ_2、增加常数值ω_2可以是预先设置的。

[0142] 通过以上的技术方案，使得本发明可以对预设评价系数进行持续的增加调整，以满足用户对目标通讯链路宽松的要求，使所得到的预设评价系数更适用于当前的计算场景。

[0143] 为了更好的实现本发明所提供的一种基于大数据日志分析的告警方法，本发明提供的技术方案还提供一种基于大数据日志分析的告警装置，如图4所示，包括：

[0144] 监测模块，用于对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志；

[0145] 比对模块，用于判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备的日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签；

[0146] 设备告警模块，用于判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则对所述串行少类标签所对应的设备运行信息及设备日志对应的通讯设备标签进行输出，进行通讯设备的告警提醒；

[0147] 链路评价模块，用于统计第二预设时间段内所进行告警提醒的串行少类标签数

量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数；

[0148] 链路告警模块，用于若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒。

[0149] 本发明还提供一种存储介质，所述存储介质中存储有计算机程序，所述计算机程序被处理器执行时用于实现上述的各种实施方式提供的方法。

[0150] 其中，存储介质可以是计算机存储介质，也可以是通信介质。通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。计算机存储介质可以是通用或专用计算机能够存取的任何可用介质。例如，存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于专用集成电路(Application Specific Integrated Circuits，简称:ASIC)中。另外，该ASIC可以位于用户设备中。当然，处理器和存储介质也可以作为分立组件存在于通信设备中。存储介质可以是只读存储器(ROM)、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0151] 本发明还提供一种程序产品，该程序产品包括执行指令，该执行指令存储在存储介质中。设备的至少一个处理器可以从存储介质读取该执行指令，至少一个处理器执行该执行指令使得设备实施上述的各种实施方式提供的方法。

[0152] 在上述终端或者服务器的实施例中，应理解，处理器可以是中央处理单元(英文:Central Processing Unit，简称:CPU)，还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor，简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit，简称:ASIC)等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0153] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案，而非对其限制;尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

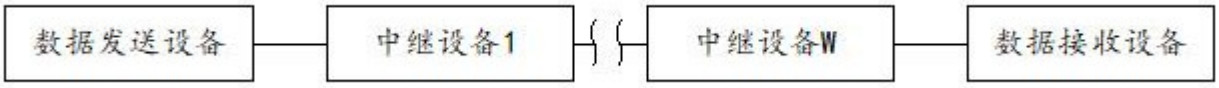

数据发送设备
中继设备1
中继设备W
数据接收设备

图1

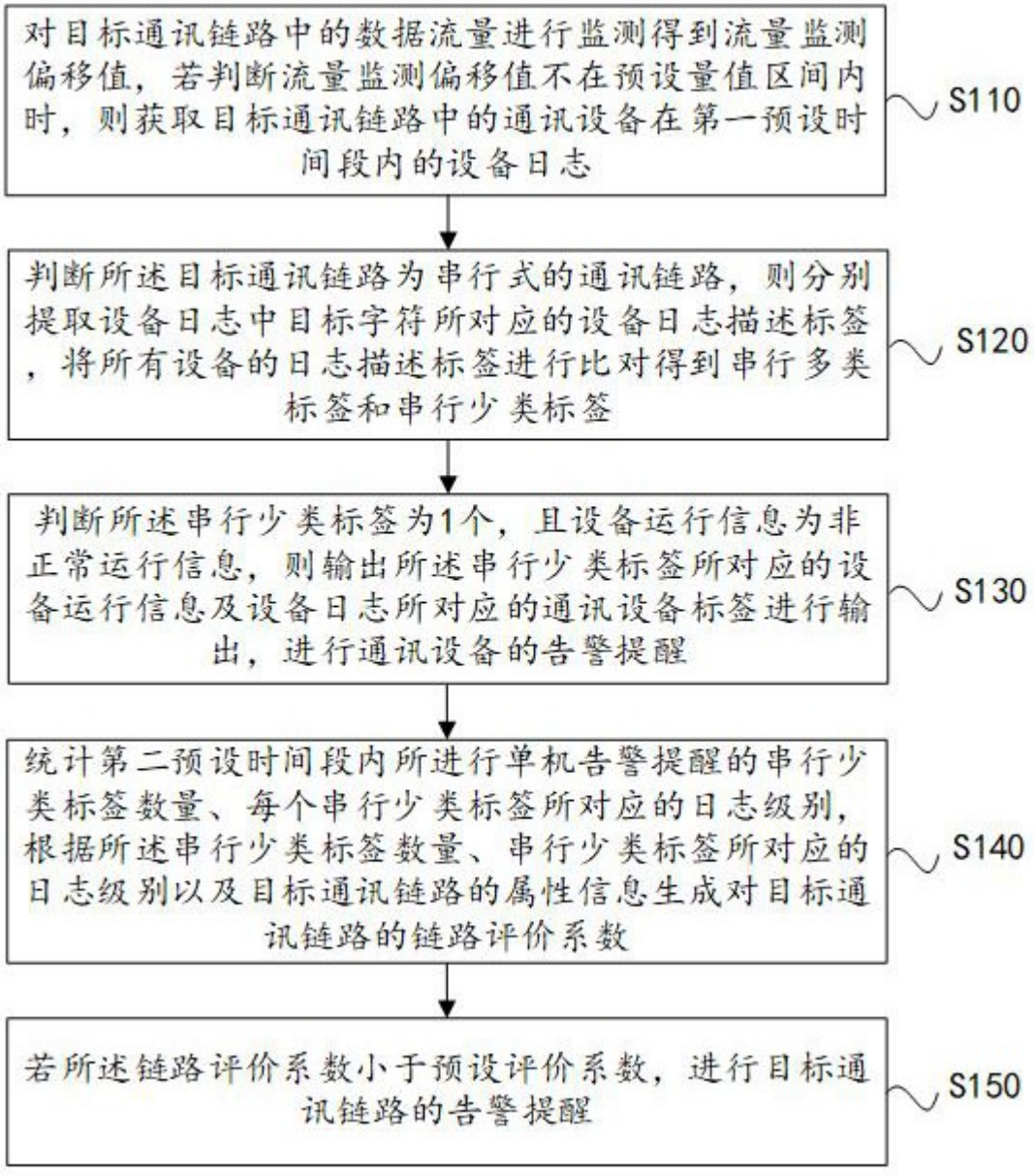

对目标通讯链路中的数据流量进行监测得到流量监测偏移值，若判断流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志
S110
判断所述目标通讯链路为串行式的通讯链路，则分别提取设备日志中目标字符所对应的设备日志描述标签，将所有设备的日志描述标签进行比对得到串行多类标签和串行少类标签
S120
判断所述串行少类标签为1个，且设备运行信息为非正常运行信息，则输出所述串行少类标签所对应的设备运行信息及设备日志所对应的通讯设备标签进行输出，进行通讯设备的告警提醒
S130
统计第二预设时间段内所进行单机告警提醒的串行少类标签数量、每个串行少类标签所对应的日志级别，根据所述串行少类标签数量、串行少类标签所对应的日志级别以及目标通讯链路的属性信息生成对目标通讯链路的链路评价系数
S140
若所述链路评价系数小于预设评价系数，进行目标通讯链路的告警提醒
S150

图2

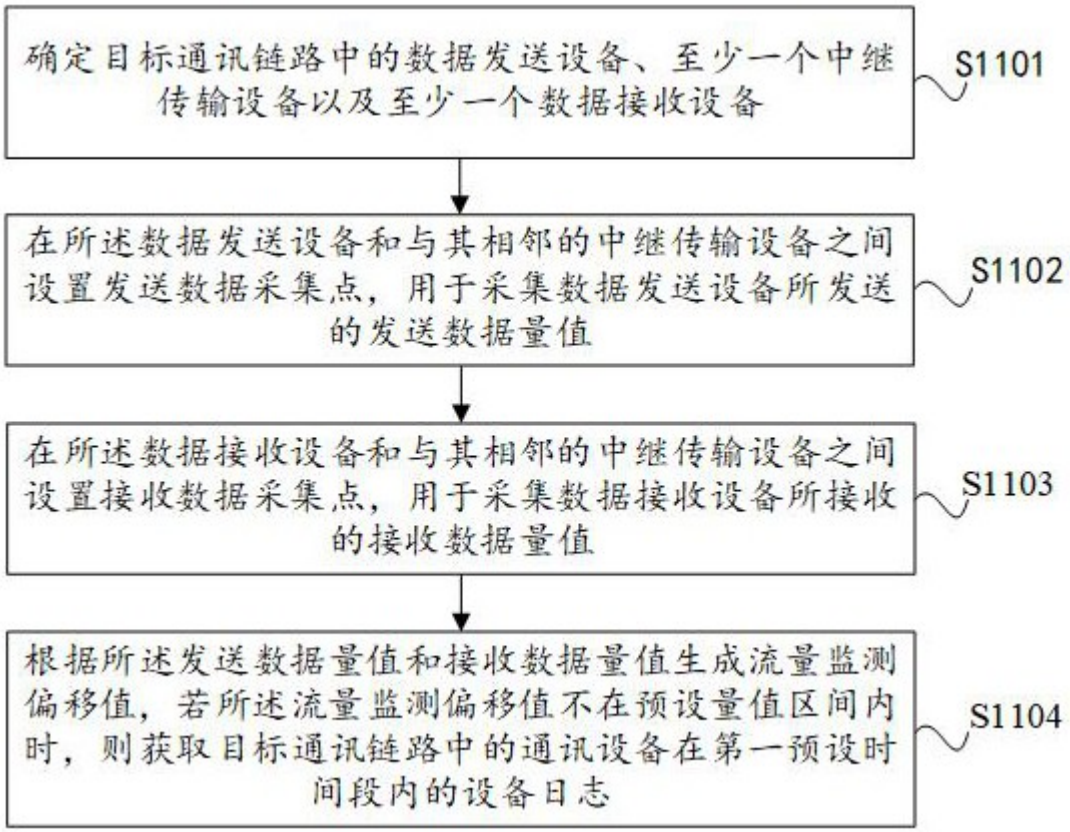

确定目标通讯链路中的数据发送设备、至少一个中继传输设备以及至少一个数据接收设备
S1101
在所述数据发送设备和与其相邻的中继传输设备之间设置发送数据采集点，用于采集数据发送设备所发送的发送数据量值
S1102
在所述数据接收设备和与其相邻的中继传输设备之间设置接收数据采集点，用于采集数据接收设备所接收的接收数据量值
S1103
根据所述发送数据量值和接收数据量值生成流量监测偏移值，若所述流量监测偏移值不在预设量值区间内时，则获取目标通讯链路中的通讯设备在第一预设时间段内的设备日志
S1104

图3

图4