(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110677324 B
(45)授权公告日 2023.02.14

(21)申请号 201910944824.7
(22)申请日 2019.09.30
(65)同一申请的已公布的文献号
申请公布号 CN 110677324 A
(43)申请公布日 2020.01.10
(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号
(72)发明人 陆以勤 彭林 覃健诚 程喆
(74)专利代理机构 广州粤高专利商标代理有限公司 44102
专利代理师 何淑珍 江裕强
(51)Int.Cl.
H04L 43/0876(2022.01)
H04L 43/08(2022.01)
H04L 43/16(2022.01)

(56)对比文件
CN 106603410 A,2017.04.26
CN 107342906 A,2017.11.10
CN 106453129 A,2017.02.22
CN 106453130 A,2017.02.22

审查员 黄倩露

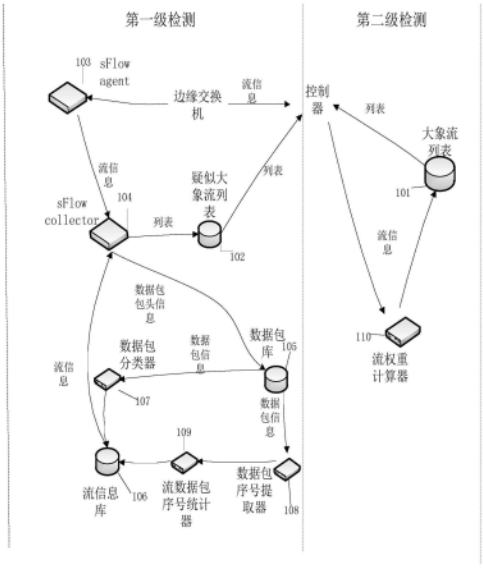
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于sFlow采样与控制器主动更新列表的大象流两级检测方法

(57)摘要

本发明公开基于sFlow采样与控制器主动更新列表的大象流两级检测方法，包括：由sFlow agent在边缘交换机随机采样数据包，将采样到的数据包信息分析并封装成一个sFlow报文，并发送到sFlow collector服务器上；由服务器计算出sFlow报文中各个流的已知字节数和数据包总数，将其中已知字节数或数据包总数超过阈值的流归为疑似大象流并将其添加到疑似大象流列表中，并发送到控制器；控制器根据服务器发送的疑似大象流列表，发送查询信息到相应的边缘交换机上，边缘交换机返回统计信息给控制器，进行权值计算，更新大象流列表。本发明解决现有检测技术中控制器与交换机通信量较大、交换机的资源消耗较大的问题。



CN 110677324 B

1.基于sFlow采样与控制器主动更新列表的大象流两级检测方法,其特征在于,该方法包括以下步骤:

S1、由sFlow agent在边缘交换机随机采样数据包,将若干个采样到的数据包信息分析并封装成一个sFlow报文,并将sFlow报文发送到sFlow collector服务器上;

S2、由sFlow collector服务器计算出sFlow报文中各个流的已知字节数和数据包总数,将其中已知字节数或数据包总数超过阈值的流归为疑似大象流并将其添加到疑似大象流列表中,将疑似大象流列表发送到控制器,完成第一级检测,具体包括:

S21、由sFlow collector服务器对接收到的sFlow报文进行分析,根据解析出来的数据信息得到源地址IP、目的地址IP、源端口、目的端口、传输层协议,将数据包进行分类,即把具有相同五元组的数据包归为同一个流;

S22、经过对采样的数据包统计得到对每个流所采样的数据包数量,再计算每个流的数据包数量与所有流的数据包总数之比,将每个流的这个比值与流占比阈值Qth比较,流占比阈值Qth可根据实际情况调整,若比值大于Qth,则将该比值大于Qth的流判定为疑似大象流,并且将其添加到疑似大象流列表中,若比值小于Qth,则将比值小于Qth的流再进行一次筛选;

S23、对于S22中得到非疑似大象流进行筛选,由sFlow collector服务器对接收到的sFlow报文进行解析,根据解析出来的数据包包头信息得到数据包的传输层协议即TCP协议,对TCP协议中TCP包的首部所包括的32位序号段进行统计并判断是否为疑似大象流,最后将疑似大象流列表发送到控制器;

S3、由控制器根据sFlow collector服务器发送的疑似大象流列表,发送查询信息到相应的边缘交换机上,边缘交换机返回统计信息,控制器对返回的信息进行权值计算,更新大象流列表,完成第二级检测。

2.根据权利要求1所述的基于sFlow采样与控制器主动更新列表的大象流两级检测方法,其特征在于,步骤S1具体包括:

在数据中心网络的边缘交换机安装sFlow agent对边缘交换机的各个端口采用sFlow采样方法进行随机采样,sFlow agent设置采样概率为1/N,即从接收的N个数据包中随机选择1个进行采样分析,sFlow agent在sFlow报文缓冲区满后,或者缓冲区未发送报文超过sec秒时,将sFlow报文发送到sFlow collector服务器上,sec可根据实际情况设定。

3.根据权利要求1所述的基于sFlow采样与控制器主动更新列表的大象流两级检测方法,其特征在于,步骤S23中对数据包中TCP序号段进行统计并判断是否为疑似大象流的具体方法为:

(1)根据五元组将数据包归类到各个流,通过将同一个流的两个数据包中的序号段相减得到字节数L,则该流的大小必然大于L个字节;在查找流中最大序列号与最小序列号时,同时比较TCP首部中的时间戳;

(2)若最大序列号的时间戳晚于最小序列号的时间戳,则没有发生序列号回绕,因此通过计算每个流的数据包中最大序号与最小序号相减得到相应的字节数Len;当发生序列号的回绕情况时,根据时间戳找出最晚的序列号S1以及最早的序列号S2,则Len＝2^32-S2+S1;

(3)将每个流的字节数L en与设定的流字节数阈值Lcom比较,流字节数阈值Lcom可调

整，若Len大于Lcom，则Len大于Lcom的流判定为疑似大象流并将其添加到疑似大象流列表中，否则判定为老鼠流，不做处理；此时第一级检测结束。

4.根据权利要求1所述的基于sFlow采样与控制器主动更新列表的大象流两级检测方法，其特征在于，步骤S3具体包括：

因为边缘交换机能提供每个流统计信息，控制器接收到sFlow collector服务器发送的疑似大象流列表后，控制器向边缘交换机发送流统计请求，边缘交换机将返回所查询流的统计信息到控制器，可以得到流的数据包数、字节数、数据流持续时间；字节数对应的权重为Wc，Wc为1/10，数据流对应的权重为Wt，Wt为1/11，则流的权重W＝字节数*Wc+流持续时间*Wt，对疑似大象流列表按权值由大到小进行排序，排在前n位的判断为大象流，n为采样所有流总数的百分之十，也可根据网络实际情况调整，由此最终筛选出大象流，此时完成第二级检测。

基于sFlow采样与控制器主动更新列表的大象流两级检测方法

技术领域

[0001] 本发明涉及到SDN数据中心网络中的流量工程技术,特别涉及一种基于sFlow采样与控制器主动更新列表的大象流两级检测方法。

背景技术

[0002] 随着SDN技术与数据中心的发展,数据中心的网络规模不断扩大,运行于网络上的流量呈爆炸式增长,拥塞问题、延迟时间、低吞吐量等问题也变得更加凸显,通过流量工程技术来优化网络资源调配对于提高网络资源利用率、降低网络成本具有重要的意义,流量工程是SDN的一类典型应用,是网络的管理者优化网络的性能和流量传输的方法,利用集中的控制来实现管理网络的转发功能以及流量调控功能。数据中心网络中存在大象流和老鼠流,大象流字节数更大、持续时间更长、更容易导致网络的拥塞影响网络性能,检测流属于哪一类流并分配相应的路径能有效的解决网络的拥塞问题。

[0003] 根据检测的位置,目前SDN中的大象流检测方法可以分为交换机检测和终端主机检测,对交换机检测可以分为两类:基于流统计的大象流检测和基于流特征的大象流检测。终端主机检测利用了主机灵活的编程性以及对流信息的早期感知,主要是基于流量统计的大象流检测。因此,现有的大象流检测技术主要包括:1、基于控制器轮询的大象流检测技术;2、基于终端标记的大象流检测技术;3、基于交换机主动检测的大象流检测技术;4、基于流采样的大象流检测技术。简单介绍如下:

[0004] 现有技术一:基于控制器轮询的大象流检测技术。

[0005] 原理:该技术通过控制器周期性的下发流统计请求到交换机上,然后交换机响应相应的流统计信息,控制器根据大象流的统计特征从所有流中筛选出大象流。

[0006] 缺点:为了保证较高的准确度,就需要最大限度地捕获网络流量,需要保持较高的轮询频率,而这样就会造成较大的监控开销,以及控制器与交换机之间的通信也会大大增加,从而影响正常的流转发。

[0007] 现有技术二:基于终端标记的大象流检测技术。

[0008] 原理:通过在终端主机上的应用程序进行大象流的检测,其中一种方法是采用基于TCP发送队列的检测方法,该方法在TCP发送队列预先对流的大小进行判断,并对判断为大象流的流进行标记,控制器在发现该标记后即可知道该流属于大象流。

[0009] 缺点:该方法虽然能较为有效的识别大象流,但是需要在所有的数据中心终端主机上部署相应的应用程序。

[0010] 现有技术三:基于交换机主动检测的大象流检测技术。

[0011] 原理:该方法是交换机在没有任何流统计请求的情况下主动向控制器发送流统计信息,与基于控制器轮询的大象流检测技术相比,可以大大的减少流量统计的监控开销。

[0012] 缺点:这种检测方法通常需要交换机的支持,需要对交换进行相应的修改,可能涉及到交换机的硬件或者软件上的修改,所以通用性较差,部署方法较为复杂。

[0013] 现有技术四:基于流采样的大象流检测技术。

[0014] 原理:该方法通常通过对交换机的各个端口进行数据包的采样,然后对采样的数据包进行统计分析然后判断哪些流属于大象流,哪些属于老鼠流;该方法的监控开销相较于其他方法较低。

[0015] 确定:该方法的检测准确度依赖于数据包的采样频率,相较于现有技术一的准确度较低。

[0016] 综上所述,现有的象流检测方法要么监控开销大,要么需要在交换机或者终端主机上进行修改,要么检测的准确度不高。

发明内容

[0017] 本发明提供的基于sFlow采样与控制器主动更新列表的大象流两级检测方法,用以解决现有大象流检测技术难以在监控开销小的情况下实现高检测准确度的问题。

[0018] 本发明的目的至少通过如下技术方案之一实现。

[0019] 一种基于sFlow采样与控制器主动更新列表的大象流两级检测方法,包括以下步骤:

[0020] S1、由sFlow agent在边缘交换机随机采样数据包,将若干个采样到的数据包信息分析并封装成一个sFlow报文,并将sFlow报文发送到sFlow collector服务器上;

[0021] S2、由sFlow collector服务器计算出sFlow报文中各个流的已知字节数和数据包总数,将其中已知字节数或数据包总数超过阈值的流归为疑似大象流并将其添加到疑似大象流列表中,将疑似大象流列表发送到控制器,完成第一级检测;

[0022] S3、由控制器根据sFlow collector服务器发送的疑似大象流列表,发送查询信息到相应的边缘交换机上,边缘交换机返回统计信息,控制器对返回的信息进行权值计算,更新大象流列表,完成第二级检测。

[0023] 具体地,步骤S1包括:

[0024] 在数据中心网络的边缘交换机安装sFlow agent对边缘交换机的各个端口采用sFlow采样方法进行随机采样,sFlow agent设置采样概率为1/N,即从接收的N个数据包中选随机择1个进行采样分析,sFlow agent在sFlow报文缓冲区满或者缓冲区未发送报文超过sec秒后时将sFlow报文发送到sFlow collector服务器上,sec可根据实际情况设定。

[0025] 具体地,步骤S2包括:

[0026] S21、由sFlow collector服务器对接收到的sFlow报文进行分析,根据解析出来的数据信息得到源地址IP、目的地址IP、源端口、目的端口、传输层协议,将数据包进行分类,即把具有相同五元组的数据包归为同一个流;

[0027] S22、经过对采样的数据包统计得到对每个流所采样的数据包数量,再计算每个流的数据包数量与所有流的数据包总数之比,将每个流的这个比值与流占比阈值Qth比较,流占比阈值Qth可根据实际情况调整,若比值大于Qth,则将比值大于Qth的流判定为疑似大象流,并且将其添加到疑似大象流列表中,若比值小于Qth,则将比值小于Qth的流进行再进行一次筛选;

[0028] S23、对于S22中得到非疑似大象流进行筛选,由sFlow collector服务器对接收到的sFlow报文进行解析,根据解析出来的数据包包头信息得到数据包的传输层协议即TCP协

议，对TCP协议中TCP包的首部所包括的32位序号段进行统计并判断是否为疑似大象流，最后将疑似大象流列表发送到控制器。

[0029] 进一步地，步骤S23中对数据包包头中TCP序号段进行统计并判断是否为疑似大象流的具体方法为：

[0030] (1)根据五元组将数据包归类到各个流，通过将同一个流的两个数据包中的序号段相减得到字节数L，则该流的大小必然大于L个字节；在查找流中最大序列号与最小序列号时，同时比较TCP首部中的时间戳；

[0031] (2)若最大序列号的时间戳晚于最小序列号的时间戳，则没有发生序列号回绕，因此通过计算每个流中数据包中最大序号与最小序号相减得到相应的字节数Len；当发生序列号的回绕情况时，根据时间戳找出最晚的序列号S1以及最早的序列号S2，则Len＝2^32-S2+S1；

[0032] (3)将每个流的字节数Len与设定的流字节数阈值Lcom比较，流字节数阈值Lcom可调整，若Len大于Lcom，则判定为疑似大象流并将其添加到疑似大象流列表中，否则判定为老鼠流，不做处理；此时第一级检测结束。

[0033] 具体地，步骤S3包括：

[0034] 控制器接收到sFlow collector服务器发送的疑似大象流列表，边缘交换机可以提供每个流统计信息，控制器向边缘交换机发送流统计请求，边缘交换机将返回所查询流的统计信息到控制器，可以得到流的数据包数、字节数、数据流持续时间；字节数对应的权重为Wc，80％的流大小小于10KB，Wc为1/10KB，数据流对应的权重为Wt，80％的流的持续时间小于11秒，Wt为1/11，则流的权重W＝字节数*Wc+流持续时间*Wt，对疑似大象流列表按权值由大到小进行排序，排在前n位的判断为大象流，n为采样所有流总数的百分之十，大象流只占总流数的10％，也可根据网络实际情况调整，由此最终筛选出大象流，此时完成第二级检测。

[0035] 与已有技术相比，本发明的有益效果体现在：

[0036] 本发明在数据包采样准确度不高的基础上，对疑似大象流通过控制器查询流信息进行进一步的筛序，进而得到更高的大象流检测准确度。

附图说明

[0037] 图1为本发明实施例提供的一种基于sFlow采样与控制器主动更新列表的大象流两级检测方法的示意图；

[0038] 图2为本发明实施例一种基于sFlow采样与控制器主动更新列表的大象流两级检测方法流程图。

具体实施方式

[0039] 针对现有大象流检测技术难以在监控开销小的情况下实现高检测准确度的问题。本发明实施例由sFlow agent在边缘交换机进行数据包随机采样，并将采样信息发送到sFlow collector服务器上；由sFlow collector服务器将计算出各个流的已知字节数或数据包总数超过阈值的流归为疑似大象流；由控制器根据sFlow collector服务器发送的疑似大象流列表，发送查询信息到相应的边缘交换机上，边缘交换机返回统计信息，控制器对

返回的信息进行权值计算，更新大象流列表，从而在数据包采样准确度不高的基础上，对疑似大象流通过控制器查询流信息进行进一步的筛序，进而得到更高的大象流检测准确度，解决了上述问题。

[0040] 实施例：

[0041] 如图1所示，一种基于sFlow采样与控制器主动更新列表的大象流两级检测方法的示意图包括：

[0042] S1、sFlow agent103采集边缘交换机的流信息，并通过sFlow报文发送到sFlow collector104，存储到数据包库105中；数据包分类器107读取到数据包库中的数据包信息，根据五元组进行流分类，并写入到流信息库106中；数据包序号提取器108提取数据包包头的序号字段，发送到流数据包序号统计器109，计算每个流的最少字节数Len，写入到流信息库106中；sFlow collector104从流信息库中读取各个流信息，筛选出疑似大象流列表102，将疑似大象流列表发送到控制器中，完成第一级检测；

[0043] S2、控制器根据疑似大象流列表查询边缘交换机的统计信息，通过流权重计算器110得到各个流的权重，根据权重进行排序，得到大象流列表101，完成第二级检测；

[0044] 如图2所示，本实施例的基于sFlow采样与控制器主动更新列表的大象流两级检测方法包括如下步骤：

[0045] 步骤201：对边缘交换机进行数据包采样，存入数据包库；

[0046] 步骤202：对数据包库中的数据包按五元组进行分类，存入流信息库中；

[0047] 步骤203：统计到的流的总数量M，变量i＝1；

[0048] 步骤204：如果i<＝M，则执行步骤205，否则转到步骤214；

[0049] 步骤205：如果流i数据包数量占采样总数的比例大于流占比阈值Qth，则转到步骤206，否则转到步骤207；

[0050] 步骤206：将流i添加到疑似大象流列表；

[0051] 步骤207：提取流i数据包包头信息的序号；

[0052] 步骤208：判断是否发生序列号的回绕情况时，是的话进行步骤210，否则进行步骤209；

[0053] 步骤209：将最大序号减去最小序号得到流i的最小下限Len；

[0054] 步骤210：根据时间戳找出最晚的序列号S1以及最早的序列号S2，则Len＝2^32-S2+S1；

[0055] 步骤211：如果Len>Lcom(流字节数阈值)，则转到步骤213；否则转到步骤212；

[0056] 步骤212：i＝i+1，转到步骤204；

[0057] 步骤213：将流i添加到疑似大象流列表，转到步骤212；

[0058] 步骤214：将疑似大象流列表发送到控制器；

[0059] 步骤215：控制器根据接受的列表发送流统计请求到边缘交换机；

[0060] 步骤216：控制器获取边缘交换机响应，得到各个流的持续时间T、字节数C；

[0061] 步骤217：计算疑似大象流的权重W＝Wt*T+Wc*C；

[0062] 步骤218：如果疑似大象流列表未遍历完，则转到步骤219；否则转到步骤220；

[0063] 步骤219：疑似大象流列表的下一个流，转到步骤217；

[0064] 步骤220：疑似大象流列表遍按权值由大到小排列；

[0065] 步骤221:取最大的n个流作为大象流列表,n为采样的所有流总数M的百分之十;

[0066] 步骤222:结束。

[0067] 通过以上的实施例的描述,本领域的技术人员可以清楚地了解到本发明可借助软件加必需的硬件平台的方式来实现。基于这样的理解,本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备执行本发明各个实施例或者实施例的某些部分所述的方法,所述计算机设备可以是个人计算机,服务器,或者网络设备等。

[0068] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

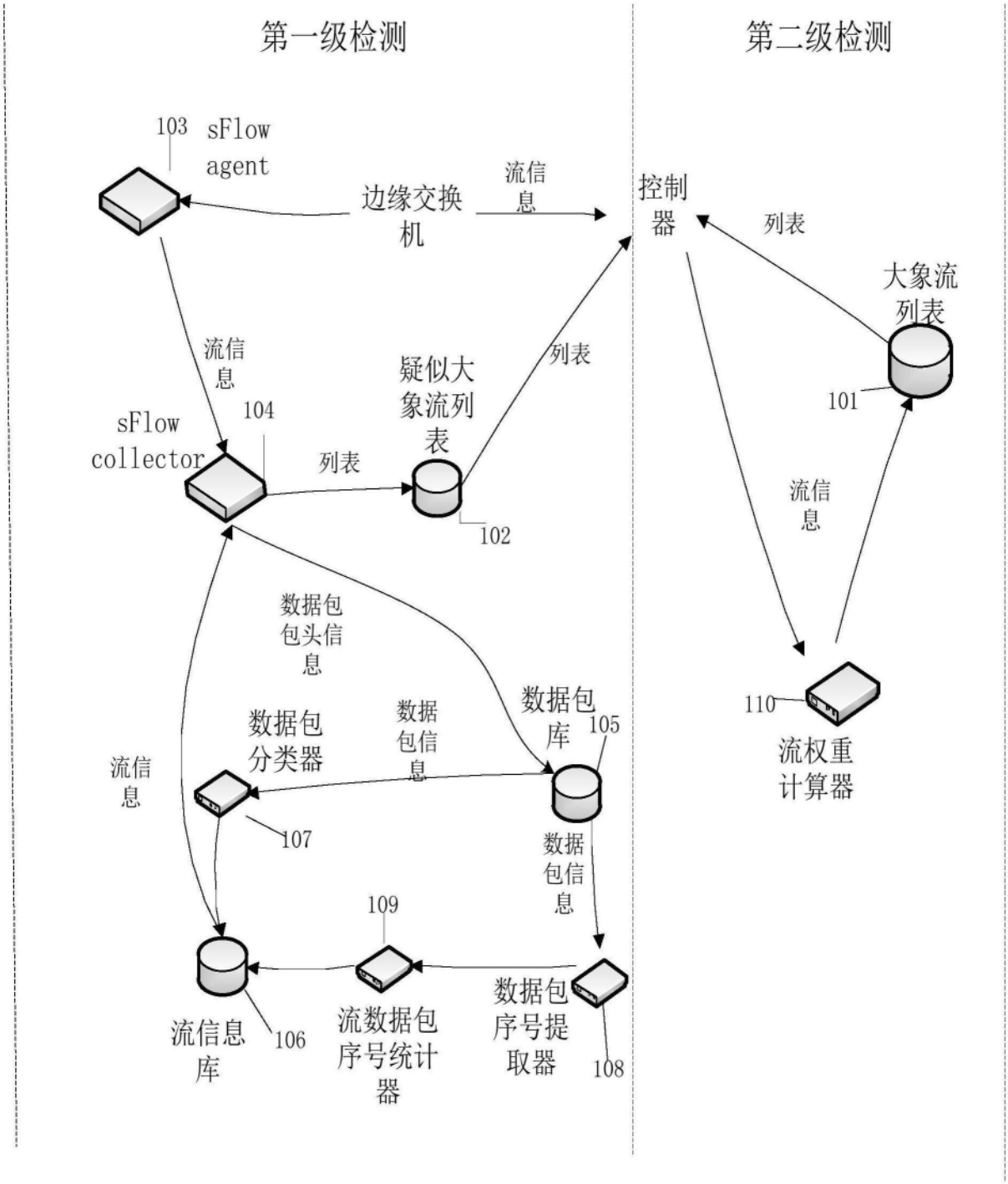

第一级检测
第二级检测
103
sFlow agent
边缘交换机
流信息
控制器
列表
大象流列表
101
流信息
104
sFlow collector
列表
疑似大象流列表
列表
102
流信息
数据包包头信息
数据包分类器
数据包信息
数据包库
105
流信息
107
数据包信息
109
流信息库
106
流数据包序号统计器
数据包序号提取器
108
110
流权重计算器

图1

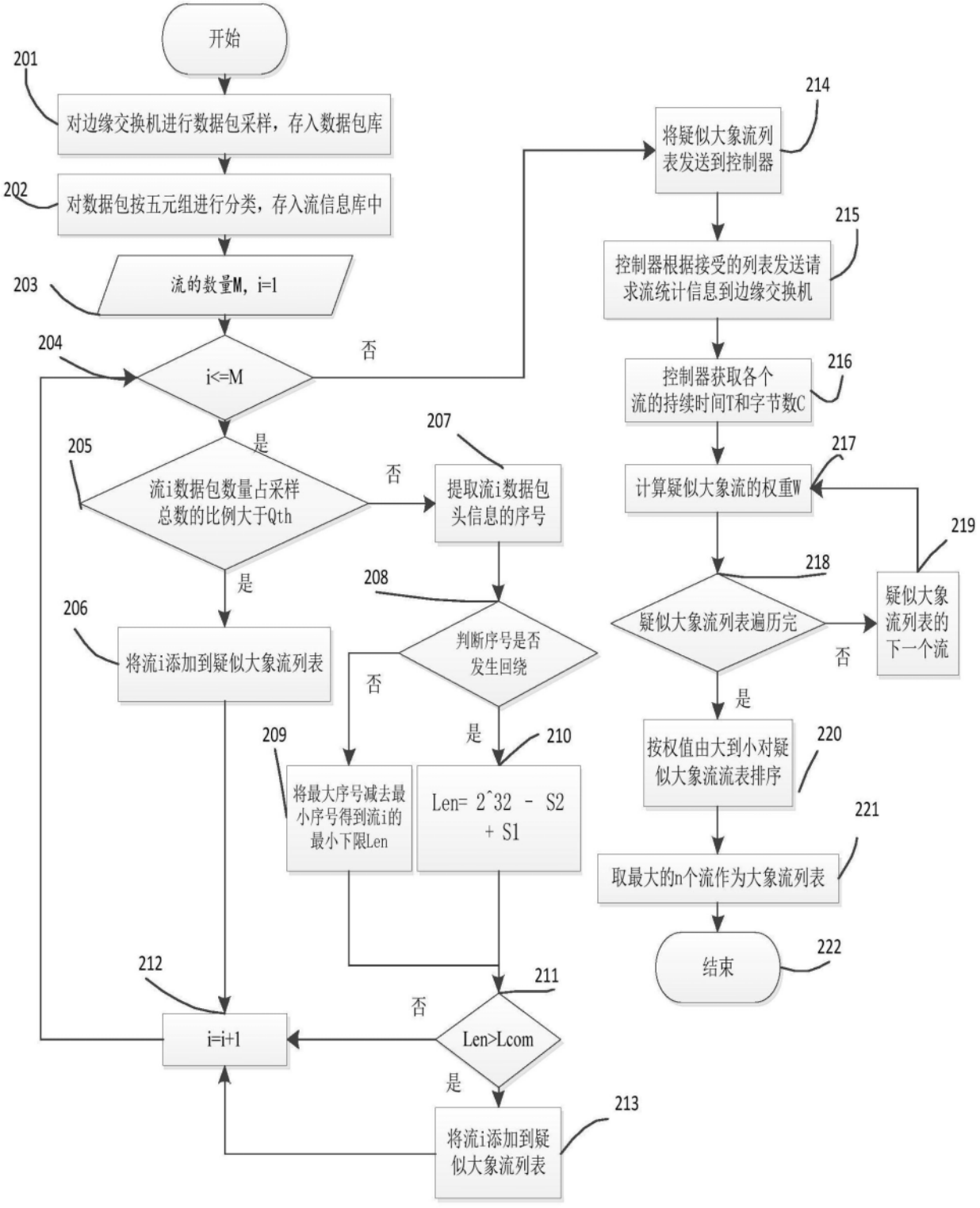

开始
201
对边缘交换机进行数据包采样，存入数据包库
202
对数据包按五元组进行分类，存入流信息库中
203
流的数量M，i=1
204
i<=M
否
是
205
流i数据包数量占采样总数的比例大于Qth
否
是
206
将流i添加到疑似大象流列表
207
提取流i数据包头信息的序号
208
判断序号是否发生回绕
否
是
209
将最大序号减去最小序号得到流i的最小下限Len
210
Len= 2^32 - S2 + S1
211
Len>Lcom
否
是
212
i=i+1
213
将流i添加到疑似大象流列表
214
将疑似大象流列表发送到控制器
215
控制器根据接受的列表发送请求流统计信息到边缘交换机
216
控制器获取各个流的持续时间T和字节数C
217
计算疑似大象流的权重W
218
疑似大象流列表遍历完
否
是
219
疑似大象流列表的下一个流
220
按权值由大到小对疑似大象流流表排序
221
取最大的n个流作为大象流列表
222
结束

图2