(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106815112 B
(45)授权公告日 2020.03.24

(21)申请号 201510850274.4

(22)申请日 2015.11.27

(65)同一申请的已公布的文献号
申请公布号 CN 106815112 A

(43)申请公布日 2017.06.09

(73)专利权人 大唐软件技术股份有限公司
地址 100012 北京市朝阳区北苑路乙108号北美国际商务中心B座

(72)发明人 杨志嘉 赵雨佳 王赟

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 11/30(2006.01)

(56)对比文件
US 2014156823 A1,2014.06.05,
CN 101364895 B,2011.05.04,
US 2014330968 A1,2014.11.06,
WO 2009021049 A3,2009.03.26,
EP 2550602 A1,2013.01.30,
CN 104796282 A,2015.07.22,

审查员 刘雨林

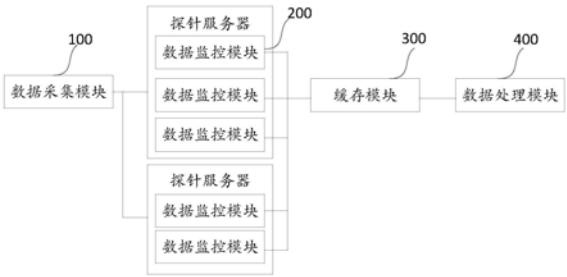
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种基于深度包检测的海量数据监控系统及方法

(57)摘要

本发明提供了一种基于深度包检测的海量数据监控系统，属于监控领域，所述系统设置有多个探针服务器，所述系统进一步包括：数据采集模块，用于按照同宿同源的规则将待监控数据分发至多个探针服务器，其中，每个所述探针服务器中设置有至少一个数据监控模块；数据监控模块，用于根据预设配置采集所述数据采集模块分发的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测；缓存模块，用于缓存所述待监控数据的识别结果和网络传输信息；数据处理模块，用于分布式存储和分析所述缓存模块发送的所述识别结果和网络传输信息，生成监控数据。与现有技术相比，可以实现高效地监控海量数据。



CN 106815112 B

1.一种基于深度包检测的海量数据监控系统,其特征在于,所述系统设置有多个探针服务器,所述系统包括:

数据采集模块,用于按照同宿同源的规则将待监控数据分发至多个探针服务器,其中,每个所述探针服务器中设置有至少一个数据监控模块;

数据监控模块,用于根据预设配置采集所述数据采集模块分发的待监控数据,并对所述待监控数据进行深度包识别和网络传输信息监测;

缓存模块,用于缓存所述待监控数据的识别结果和网络传输信息;

数据处理模块,用于分布式存储和分析所述识别结果和网络传输信息,生成监控数据。

2.如权利要求1所述的系统,其特征在于,所述预设配置包括所述数据监控模块的部署编号和所述探针服务器上采集所述待监控数据的网卡标识,

所述数据监控模块进一步用于,采集所述网卡标识指定的网卡接收的待监控数据,并对所述待监控数据进行深度包识别和网络传输信息监测。

3.如权利要求2所述的系统,其特征在于,所述数据监控模块进一步包括:

流量读取模块,用于实时采集所述网卡标识指定的网卡接收的所述待监控数据,根据网络层协议和传输层协议对所述待监控数据进行解析并封装成待识别数据包;

业务数据提取模块,用于解析所述待识别数据包,提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息;

识别模块,用于加载业务类型识别引擎识别所述业务数据的应用类型,以及监测与所述应用类型关联的所述业务数据的网络传输信息;

统计模块,用于统计并存储所述业务数据的网络传输信息;

缓存接口模块,用于建立和缓存服务器的连接池,并根据调用从所述连接池中选择空闲连接,将所述业务数据的识别结果和网络传输信息存储至所述缓存模块;

设定数量的工作线程,用于依次调用所述业务数据提取模块、识别模块、统计模块,对所述流量读取模块封装的待识别数据包进行深度包识别和网络传输信息监测,再调用所述缓存接口模块提供的接口存储所述待监控数据的识别结果和网络传输信息。

4.如权利要求3所述的系统,其特征在于,所述识别模块进一步包括:多个设置有不同调用优先级的业务类型识别引擎,所述识别模块按照调用优先级由高到低的顺序依次加载所述业务类型识别引擎识别所述业务数据的应用类型,以及监测所述应用类型关联的所述业务数据的网络传输信息。

5.如权利要求1至4任意一项权利要求所述的系统,其特征在于,所述缓存模块采用键值对的方式缓存所述待监控数据的识别结果和网络传输信息,其中,键值为所述待监控数据的时间戳和五元组,值为所述待监控数据的识别结果和网络传输信息;

所述系统进一步包括:数据转发模块,用于对缓存模块缓存的所述识别结果和网络传输信息进行格式转换,并发送至所述数据处理模块。

6.一种基于深度包检测的海量数据监控方法,其特征在于,预设多个探针服务器,所述方法包括:

按照同宿同源的规则将待监控数据分发至所述多个探针服务器;

根据预设配置在每个所述探针服务器上创建多个数据监控实例;

根据预设配置采集分发至当前探针服务器的所述待监控数据,并对所述待监控数据进

行深度包识别和网络传输信息监测；

缓存所述待监控数据的识别结果和网络传输信息；

分布式存储和分析所述识别结果和网络传输信息，生成监控数据。

7.如权利要求6所述的方法，其特征在于，所述预设配置包括所述数据监控实例的部署编号和所述探针服务器上采集所述待监控数据的网卡标识，

所述根据预设配置创建多个数据监控实例，进一步包括：根据所述数据监控实例的部署编号创建多个数据监控实例；

所述根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测的步骤，进一步包括，采集所述网卡标识指定的网卡接收的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测。

8.如权利要求7所述的方法，其特征在于，所述根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测的步骤，进一步包括：

实时采集所述网卡标识指定的网卡接收的待监控数据，根据网络层协议和传输层协议对所述待监控数据进行解析并封装成待识别数据包；

根据预设配置创建设定数量的工作线程；

启动所述工作线程，解析封装的所述待识别数据包，提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息；加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息；统计并存储所述业务数据的网络传输信息；再调用缓存接口从预先建立的与缓存服务器的连接池中选择空闲连接，存储所述业务数据的识别结果和网络传输信息。

9.如权利要求8所述的方法，其特征在于，所述方法还包括，预先设置多个不同调用优先级的业务类型识别引擎，

所述加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，进一步包括：按照调用优先级由高到低的顺序依次加载所述业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息。

10.如权利要求6至9任意一项权利要求所述的方法，其特征在于，采用键值对的方式缓存所述待监控数据的识别结果和网络传输信息，其中，键值为所述待监控数据的时间戳和五元组，值为所述待监控数据的识别结果和网络传输信息；

所述方法进一步包括：对缓存的所述识别结果和网络传输信息进行格式转换并转发。

一种基于深度包检测的海量数据监控系统及方法

技术领域

[0001] 本发明涉及数据监控领域，特别是涉及一种基于深度包检测的海量数据监控系统及方法。

背景技术

[0002] 随着互联网技术的不断发展，网络已经渗透到了国家的政治、经济、军事、文化、生活等各个领域，整个社会的运转已经与网络密不可分。这种对网络的高度依赖性，使得网络的稳定与安全成为一个需要重点关注和解决的问题。为了实现网络的稳定与安全运行，现有技术中通常会利用网络检测技术来识别网络传输信息的安全性、分析网络流量异常等。例如，常用的DPI(deep package inspection深度报文检测)技术，是一种面向应用层的流量分析检测技术，可实现对网络流量的深度检测分析。现有技术中的DPI技术的应用场景是针对运营商、企业、校园、网吧等，将DPI软件设置于以太网交换机或路由器中，用于流量的识别和监控处理。

[0003] 然而，随着互联网技术的不断发展，网络传输的数据量不断增加，现有的DPI软件受其运算性能的限制，仅能监控数据量小的以太网络的流量，无法实现对于运营商多个骨干网络传输的海量数据进行同时监控。

[0004] 因此，如何高效地监控运营商骨干网络中传输的海量数据成为一个急待解决的问题。

发明内容

[0005] 本申请所要解决的技术问题是：提供一种基于深度包检测的海量数据监控方法和系统，解决高效地监控运营商骨干网络中传输的海量数据的问题。

[0006] 为了解决上述问题，本发明实施例提供了一种基于深度包检测的海量数据监控系统，所述系统设置有多个探针服务器，所述系统包括：

[0007] 数据采集模块，用于按照同宿同源的规则将待监控数据分发至多个探针服务器，其中，每个所述探针服务器中设置有至少一个数据监控模块；

[0008] 数据监控模块，用于根据预设配置采集所述数据采集模块分发的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测；

[0009] 缓存模块，用于缓存所述待监控数据的识别结果和网络传输信息；

[0010] 数据处理模块，用于分布式存储和分析所述识别结果和网络传输信息，生成监控数据。

[0011] 本发明的一个实施例中，所述预设配置包括所述数据监控模块的部署编号和所述探针服务器上采集所述待监控数据的网卡标识，

[0012] 所述数据监控模块进一步用于，采集所述网卡标识指定的网卡接收的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测。

[0013] 具体实施时，本发明的另一实施例中，所述数据监控模块进一步包括：

[0014] 流量读取模块，用于实时采集所述网卡标识指定的网卡接收的所述待监控数据，根据网络层协议和传输层协议对所述待监控数据进行解析并封装成待识别数据包；

[0015] 业务数据提取模块，用于解析所述待识别数据包，提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息；

[0016] 识别模块，用于加载业务类型识别引擎识别所述业务数据的应用类型，以及监测与所述应用类型关联的所述业务数据的网络传输信息；

[0017] 统计模块，用于统计并存储所述业务数据的网络传输信息；

[0018] 缓存接口模块，用于建立和缓存服务器的连接池，并根据调用从所述连接池中选择空闲连接，将所述业务数据的识别结果和网络传输信息存储至所述缓存模块；

[0019] 设定数量的工作线程，用于依次调用所述业务数据提取模块、识别模块、统计模块，对所述流量读取模块封装的待识别数据包进行深度包识别和网络传输信息监测，再调用所述缓存接口模块提供的接口存储所述待监控数据的识别结果和网络传输信息。

[0020] 优选地，所述识别模块进一步包括：多个设置有不同调用优先级的业务类型识别引擎，所述识别模块按照调用优先级由高到低的顺序依次加载所述业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息。

[0021] 本发明的再一实施例中，基于前述实施例，所述缓存模块采用键值对的方式缓存所述待监控数据的识别结果和网络传输信息，其中，键值为所述待监控数据的时间戳和五元组，值为所述待监控数据的识别结果和网络传输信息；

[0022] 所述系统进一步包括：数据转发模块，用于对缓存模块缓存的所述识别结果和网络传输信息进行格式转换，并发送至所述数据处理模块。

[0023] 相应地，本发明还公开了一种基于深度包检测的海量数据监控方法，预设多个探针服务器，所述方法包括：

[0024] 按照同宿同源的规则将待监控数据分发至所述多个探针服务器；

[0025] 根据预设配置在每个所述探针服务器上创建多个数据监控实例；

[0026] 根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测；

[0027] 缓存所述待监控数据的识别结果和网络传输信息；

[0028] 分布式存储和分析所述识别结果和网络传输信息，生成监控数据。

[0029] 在本发明的一个实施例中，所述预设配置包括所述数据监控实例的部署编号和所述探针服务器上采集所述待监控数据的网卡标识，

[0030] 所述根据预设配置创建多个数据监控实例，进一步包括：根据所述数据监控实例的部署编号创建多个数据监控实例；

[0031] 所述根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测的步骤，进一步包括，采集所述网卡标识指定的网卡接收的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测。

[0032] 具体实施时，本方明的另一实施例中，所述根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测的步骤，进一步包括：

[0033] 实时采集所述网卡标识指定的网卡接收的待监控数据，根据网络层协议和传输层

协议对所述待监控数据进行解析并封装成待识别数据包；

[0034] 根据预设配置创建设定数量的工作线程；

[0035] 启动所述工作线程，解析封装的所述待识别数据包，提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息；加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息；统计并存储所述业务数据的网络传输信息；再调用缓存接口从预先建立的与缓存服务器的连接池中选择空闲连接，存储所述业务数据的识别结果和网络传输信息。

[0036] 优选地，所述方法还包括，预先设置多个不同调用优先级的业务类型识别引擎，

[0037] 所述加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，进一步包括：按照调用优先级由高到低的顺序依次加载所述业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息。

[0038] 基于前述实施例，本发明的又一实施例中，采用键值对的方式缓存所述待监控数据的识别结果和网络传输信息，其中，键值为所述待监控数据的时间戳和五元组，值为所述待监控数据的识别结果和网络传输信息；

[0039] 所述方法进一步包括：对缓存的所述识别结果和网络传输信息进行格式转换并转发。

[0040] 本发明实施例通过按照同宿同源的规则将待监控的海量数据分发至多个探针服务器，然后，在每个所述探针服务器中设置有至少一个数据监控模块；利用所述数据监控模块根据预设配置采集所述数据采集模块分发的待监控数据，并进行深度包识别和网络传输信息监测；最后通过缓存系统发送至大数据平台进行分析，有效地解决了现有技术中DPI技术无法实现海量数据检测的问题，高效地实现了海量数据的监控。

附图说明

[0041] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术描述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。

[0042] 图1是本发明一个实施例的基于深度包检测的海量数据监控系统的结构图；

[0043] 图2是本发明另一实施例的基于深度包检测的海量数据监控系统的数据监控模块的结构图；

[0044] 图3是本发明又一实施例的基于深度包检测的海量数据监控系统的结构图；

[0045] 图4是本发明一个实施例的基于深度包检测的海量数据监控方法的流程图；

[0046] 图5是本发明另一实施例的基于深度包检测的海量数据监控方法的流程图。

具体实施方式

[0047] 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作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。

[0048] 为了使阅读者更容易理解本发明，下面先对本发明中涉及的专业术语进行介绍：

[0049] 五元组，指源IP地址、源端口、目的IP地址、目的端口、和传输层协议这五个量组成的一个集合。例如：192.168.1.1 10000 TCP 121.14.88.76 80就构成了一个五元组。其意义是，一个IP地址为192.168.1.1的终端通过端口10000，利用TCP协议，和IP地址为121.14.88.76，端口为80的终端进行连接。

[0050] 深度包检测技术即DPI(Deep Packet Inspection)技术是一种基于应用层的流量检测和控制技术，当IP数据包、TCP或UDP数据流通过基于深度包检测技术的带宽管理系统时，该系统通过深入读取IP包载荷的内容来对OSI七层协议中的应用层信息进行分析，从而得到整个应用程序的内容，实现流量监控等应用。

[0051] 实施例一：

[0052] 本发明实施例公开了一种基于深度包检测的海量数据监控系统，包括多个探针服务器，如图1所示，所述系统包括：

[0053] 数据采集模块100，用于按照同宿同源的规则将待监控数据分发至多个探针服务器，其中，每个所述探针服务器中设置有至少一个数据监控模块200；

[0054] 数据监控模块200，用于根据预设配置采集所述数据采集模块100分发的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测

[0055] 缓存模块300，用于缓存所述待监控数据的识别结果和网络传输信息；

[0056] 数据处理模块400，用于分布式存储和分析所述识别结果和网络传输信息，生成监控数据。

[0057] 其中，所述识别结果包括所述待监控数据的应用类型，所述网络传输信息包括：流量、IP分片信息、TCP重传率等。所述待监控数据的应用类型包括根据网络层协议和传输层协议对所述待监控数据进行解析后得到的业务数据的应用类型。

[0058] 下面分别介绍各个模块的具体实施方式。

[0059] 流量采集可以采用旁路部署或者串接部署方式，实现对网络流量的镜像分流。具体实施时，本实施例采用旁路部署方式，实现在不影响原有网络运行的情况下，对网络流量的镜像分流。将流量采集模块100部署至运营商骨干网络的各个路由器中。流量采集模块100可以是一个分流设备，按照一定的规则将同一会话的报文分流至同一个探针服务器。本实施例中，在海量数据通过运营商的骨干网络进行传输时，所述流量采集模块100获取每一个骨干网络的镜像流量，然后，按照同宿同源的原则将采集的网络流量分发到各个探针服务器上。例如，按照源IP地址和目标IP地址相同的原则，将源IP地址和目标IP地址相同的网络流量发送至同一个探针服务器，并由设置在该探针服务器上的同一个数据监控模块进行处理，可以提高流量监控的效率。通过将采集的流量进行分流处理，可以通过扩展探针服务器来实现海量数据的流量采集。

[0060] 所述探针服务器可以为PC机等具有网络传输能力的任何运算设备。所述探针服务器上设置有至少一块用于采集待监测数据流量的网卡，用于接收数据采集模块100分发的待监控数据。

[0061] 每个所述探针服务器中设置有至少一个数据监控模块200。在进行数据检测之前，所述探针服务器还设置有配置文件和协议文件，存储所述数据监控模块200执行所需要的

基本信息，用于配置所述数据监控模块200。所述数据监控模块200进一步包括：初始化模块2001、流量读取模块2002、多个工作线程2003、业务数据提取模块2004、识别模块2005、统计模块2006、缓存接口模块2007、日志模块2008，如图2所示。其中，业务数据提取模块2004进一步包括：IP模块、TCP模块。所述配置文件中包括：数据监控模块200的部署编号、采集所述待监控数据的网卡标识(即需要监听的网卡标识)、工作线程数量、日志文件存储路径、缓存服务器的IP地址和端口等信息。协议文件中包括：应用的特征信息，比如网站域名、协议名称、等字符串信息，或端口号、特定的Bit序列等二进制特征。每一个数据监控模块200有一个唯一的部署编号，数据监控模块200运行时，创建一个数据监控运行实例，该部署编号用来标记所述数据监控实例。所述数据监控模块200进一步用于，采集所述网卡标识指定的网卡接收的待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测。

[0062] 初始化模块2001用于根据配置文件中的内容初始化流量读取模块2002、工作线程2003、缓存接口模块2007；根据协议文件的内容初始化识别模块2005。具体实施时，初始化模块2001读取配置文件中的网卡标识初始化流量读取模块2002，完成监听该网卡标识对应的网卡的初始化工作；根据工作线程数量创建相应个数的工作线程2003；根据缓存服务器的IP地址和端口和缓存服务器集群建立连接，并进一步建立和缓存服务器集群的连接池，用于其他各模块调用缓存服务器集群提供的接口。初始化模块2001还用于读取协议文件中的特征信息，根据协议文件中的特征建立字典树，便于识别模块2005在进行协议识别时进行快速查询匹配。初始化模块2001还用于初始化业务数据提取模块2004，如：IP模块、TCP模块。其中，初始化IP模块进一步包括：创建一个用于存储IP分组信息的hash表，所述hash表中至少存储IP分组的报文头部。所述IP分组信息包括IP分组的报文头部，用于区分分组和判断分组是否分片。初始化TCP模块进一步包括：创建一个用于存储TCP会话状态的hash表。初始化模块2001还用于初始化统计模块2006，如分配阈值大小的存储空间用于缓存各模块生成的数据包相关信息的统计记录。

[0063] 数据监控模块200的初始化工作完成之后，即调用流量读取模块2002开始工作，并启动所述工作线程2003。

[0064] 所述流量读取模块2002用于实时采集所述网卡标识指定的网卡接收的待监控数据，根据网络层协议(IP协议)和传输层协议(TCP协议)对所述待监控数据进行解析并封装成待识别数据包。具体实施时，流量读取模块2002实时读取指定的网卡的数据，根据链路层协议解析为IP分组数据，然后根据IP协议规定，将数据解析为对应的传输层协议数据，最后把解析结果封装成待识别数据包，交给下一个模块使用。所述待识别数据包中包括：数据包的长度，各层数据的起始位置，状态、业务数据等。

[0065] 每个所述工作线程2003，用于依次调用业务数据提取模块2004、识别模块2005、统计模块2006，对流量读取模块2002封装的待识别数据包进行深度包识别和网络传输信息监测，最后，调用缓存接口模块2007提供的接口，将所述业务数据提取模块2004、识别模块2005、统计模块2006获得的所述待监控数据的识别结果和网络传输信息进行缓存。

[0066] 业务数据提取模块2004用于解析所述流量读取模块2002封装的待识别数据包，提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息。其中，所述IP模块用于对所述流量读取模块封装的待识别数据包进行分组及重组得到TCP数据包，以及监控IP层相关信息，如IP分片信息。具体实现过程如下：分析所述待识别数据包的报文头部，

报文头部里面有报文编号和是否分组的标记，将分析得到的报文头部存储至hash表中，同时，将同一分组的报文编号存储在hash表中，以实现报文重组得到TCP数据。IP模块还用于监控IP层相关信息，如IP分片信息。

[0067] TCP模块用于解析IP模块生成的TCP数据包，实现TCP会话的重组以及监控TCP层相关信息。具体实现过程如下：TCP报文头部包含了编号和一些状态控制信息。从流量包中将这些信息分析出来后，得到TCP本流量包中的TCP会话信息，根据该信息更新hash表中该会话的状态，实现会话的重组，得到业务数据。同时，统计TCP重传率，并将获得的TCP重传率等数据通过调用缓存接口模块的接口进行缓存。

[0068] 识别模块2005用于加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息。其中，所述业务类型识别引擎可以为基于深度包检测的识别软件。所述识别模块2005首先调用业务类型识别引擎，根据预先初始化的字典树识别业务数据的应用类型，并根据识别的应用类型，进一步进行监控数据提取，得到该应用类型对应的监控数据。例如，当识别模块2005调用业务类型识别引擎识别出当前待识别数据包为HTTP协议应用后，根据识别的应用类型，进一步进行数据监测，得到该应用类型对应的监控数据。例如，进一步提取当前业务数据中的URL、数据流量等HTTP协议类型的业务数据的具体监控信息。识别模块2005识别得到业务数据的应用类型后，工作线程2003将业务数据的流量大小发送至统计模块2006进行统计。

[0069] 所述统计模块2006，用于统计并存储所述业务数据的网络传输信息，如用于存储各个应用类型的待监控数据的流量信息，对于已经识别的流量，计算其大小，更新记录的统计数据。

[0070] 所述缓存接口模块2007用于建立和缓存服务器的连接池，并根据各个工作线程2003的调用，从所述连接池中选择空闲连接，将所述业务数据的识别结果和网络传输信息存储至所述缓存模块300。

[0071] 日志模块2008用于存储、维护日志文件。日志文件存储在探针服务器的本地磁盘上，在需要的时候便于对数据监控模块200的运行状态的监督查看。根据磁盘空间进行定时清理。日志模块2008通过封装文件读写操作，为各个模块提供日志保存的读取的接口。初始化模块2001、流量读取模块2002、各工作线程2003、业务数据提取模块2004、识别模块2005等在执行过程中实时保存操作日志，便于数据监控系统的维护和工作状态查询。

[0072] 缓存模块300用于缓存所述待监控数据的识别结果和网络传输信息，包括：待监控数据的识别结果和统计数据。缓存模块300采用快速的内存数据库实现，例如，采用Redis内存数据库集群。

[0073] 具体实施时，优选地，缓存模块300采用键值对(Key-Value)的方式存储业务数据的识别结果，其中，键值(Key)为：待监控数据的时间戳和五元组，值(Value)为所述待监控数据的识别结果和网络传输信息，如待监控数据的基本应用类型、流量等数据。在数据监控模块识别出待识别数据包的五元组和基本应用类型后，直接将识别结果和识别结果的统计数据提交到Redis数据库集群，方便、快捷。采用键值对的方式存储数据包的识别结果，并且用数据包的时间戳和五元组作为Key，用识别结果作为Value，便于数据监控模块进行快速存储。

[0074] 数据处理模块400用于分布式存储和分析所述识别结果和网络传输信息，生成监

控数据。具体实施时，数据处理模块400可以采用大数据平台，数据监控模块200的数据包识别结果和数据监测结果存储在大数据平台的分布式存储系统中；由大数据平台的分布式计算系统实现对海量数据的统计分析工作，实现对大流量数据的监控。大数据平台可以选用Hadoop平台，使用HDFS作为分布式存储系统，使用HBase存储由缓存模块输出的数据包识别结果和统计数据。采用HBase进行数据存储后，同样支持使用Map/Reduce进行大数据的离线处理。另外，对于需要实时对数据包识别结果进行检测的应用场景中，例如：需要监控实时流量、实时应用排名等数据时，采用Storm实现实时处理，更新统计结果。

[0075] 通过采用大数据平台，可以实现海量数据的分析。例如，利用大数据平台的分布式计算能力，根据分布式存储系统中存储的HTTP业务的IP地址信息、流量信息、URL信息等，统计某一地区访问特定网站的次数；统计各个网路节点的流量大小丢包重传率等网络服务质量；统计业务流量排名；透过DNS记录发现DDOS攻击等。

[0076] 缓存模块300和数据处理模块400的存储结构是不一样的，具体实施时，如图3所示，所述数据监控系统还包括：数据转发模块500，用于对缓存模块300缓存的所述识别结果和网络传输信息进行格式转换，并发送至所述数据处理模块400进行分布式存储和分析。

[0077] 本发明实施例通过按照同宿同源的规则将待监控的海量数据分发至多个探针服务器，然后，在每个所述探针服务器中设置有至少一个数据监控模块；利用所述数据监控模块根据预设配置采集所述数据采集模块分发的待监控数据，并进行深度包识别和网络传输信息监测；最后通过缓存系统发送至大数据平台进行分析，有效地解决了现有技术中DPI技术无法实现海量数据检测的问题，高效地实现了海量数据的监控。

[0078] 实施例二：

[0079] 基于前述实施例一，本发明的另一优选实施例中，为了提升识别速度，所述识别模块2005设置多个业务类型识别引擎，根据业务类型的使用频率，各业务类型识别引擎设置有不同的调用优先级，使用频率高的业务类型对应的识别引擎优先调用。识别模块2005按照优先级由高到低的顺序依次调用各业务类型识别引擎，识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，直至完成识别。所述业务类型识别引擎包括：会话匹配引擎、端口识别引擎、HTTP引擎、TCP引擎、UDP引擎、DNS识别引擎、SMTP识别引擎、聊天类应用识别引擎等等。不同的业务类型识别引擎识别的具体内容不同。

[0080] 具体实施时，例如：会话识别引擎的优先权为1、端口识别引擎的优先权为2、HTTP引擎的优先权为3、TCP引擎的优先权为4、UDP引擎的优先权为5，数字越小优先权越高。当工作线程2003获取流量读取模块2002生成的待识别数据包后，调用业务数据提取模块2004提取其中的业务数据；然后，调用到识别模块2005对业务数据的业务类型进行识别。在进行业务类型识别时，首先调用会话识别引擎。如果识别成功，则返回业务类型，其中，会话识别引擎会记录已识别会话的业务类型，如果待识别数据包属于已识别会话，则默认该数据包是该会话已记录的业务类型。若会话识别引擎识别失败，则继续调用端口识别引擎；若所述端口识别引擎识别失败，则继续调用HTTP引擎，直至识别出当前业务数据的业务类型。

[0081] 业务类型识别模块识别成功后，根据识别的应用类型，进一步进行监控数据提取，得到该应用类型对应的监控数据。例如，HTTP引擎识别出当前业务数据为HTTP协议数据，则确定当前数据包的业务类型为HTTP协议类型，HTTP引擎进一步提取当前业务数据中的URL、

数据流量等HTTP协议类型的业务数据的具体监控信息。

[0082] 本发明的实施例通过根据业务类型的使用频率，各业务类型识别引擎设置有不同的调用优先级，并按照优先级由高到低的顺序依次调用各业务类型识别引擎，识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，可以提高识别效率。

[0083] 实施例三：

[0084] 相应地，本发明还公开了一种基于深度包检测的海量数据处理方法，预设多个探针服务器，如图4所示，包括：

[0085] 步骤400，按照同宿同源的规则将待监控数据分发至所述多个探针服务器；

[0086] 步骤410，根据预设配置在每个所述探针服务器上创建多个数据监控实例；

[0087] 步骤420，根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测；

[0088] 步骤430，缓存所述待监控数据的识别结果和网络传输信息；

[0089] 步骤440，分布式存储和分析所述识别结果和网络传输信息，生成监控数据。

[0090] 步骤400中，通过网络分流设备，按照同宿同源的规则将待监控数据分发至多个探针服务器。在所述探针服务器预设有配置文件和协议文件，其中，所述配置文件中包括：数据监控实例的部署编号、采集所述待监控数据的网卡标识(即需要监听的网卡标识)、工作线程数量、日志文件存储路径、缓存服务器的IP地址和端口等信息。协议文件中包括：应用的特征信息，比如网站域名、协议名称、等字符串信息，或端口号、特定的Bit序列等二进制特征。

[0091] 所述步骤410进一步包括：根据所述数据监控实例的部署编号创建多个数据监控实例，每一个部署编号对应一个数据监控实例。具体实施时，监控实例可以为DPI软件。

[0092] 所述步骤420，进一步包括，采集所述网卡标识指定的网卡接收的待监控数据，并进行深度包识别和网络传输信息监测。即每一个数据监控实例对一个网卡采集的数据进行数据监控。

[0093] 具体实施时，所述步骤420，进一步包括：

[0094] 步骤4202，实时采集所述网卡标识指定的网卡接收的待监控数据，根据网络层协议和传输层协议对所述待监控数据进行解析并封装成待识别数据包；

[0095] 步骤4203，根据预设配置创建设定数量的工作线程；

[0096] 步骤4204，启动所述工作线程，解析封装的所述待识别数据包，提取所述待识别数据包中的业务数据并监测所述业务数据的网络传输信息；加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息；统计并存储所述业务数据的网络传输信息；再调用缓存接口从预先建立的与缓存服务器的连接池中选择空闲连接，存储所述业务数据的识别结果和网络传输信息。

[0097] 上述步骤4202的具体实现过程参见实施例一的业务数据提取模块，此处不再赘述。

[0098] 步骤4203中，根据预先设置的工作线程的数量，创建相应数量的工作线程，其中工作线程的数量根据探针服务器的CPU处理能力，由预设的配置文件中指定。

[0099] 步骤4204中，启动各工作线程，进行待监控数据的深度包识别和待监控数据的网

络传输信息的监测。具体实施时，首先，实时采集所述网卡标识指定的网卡接收的待监控数据，根据网络层协议和TCP协议对所述待监控数据进行解析并封装成待识别数据包。具体实施时，实时读取指定的网卡的数据，根据链路层协议解析为IP分组数据，然后根据网络层协议(IP协议)规定，将数据解析为对应的传输层协议数据，再把解析结果封装成待识别数据包所述待识别数据包中包括：数据包的长度，各层数据的起始位置，状态、业务数据等。然后，加载业务类型识别引擎识别所述待识别数据包的应用类型，以及监测所述待识别数据包中所述应用类型关联的所述业务数据的网络传输信息；再后，统计并存储所述业务数据的网络传输信息；最后，调用缓存接口从预先建立的与缓存服务器的连接池中选择空闲连接，存储所述业务数据的识别结果和网络传输信息。

[0100] 所述步骤420中，在步骤4201之前，还包括步骤4200，根据配置文件中的内容完成监听该网卡标识对应的网卡的初始化工作、创建一个用于存储IP分组信息的hash表、创建一个用于存储TCP会话状态的hash表、建立和缓存服务器的连接；根据协议文件中的特征建立字典树，用于识别数据的应用类型。

[0101] 上述步骤430中，具体实施时，优选地，采用键值对(Key-Value)的方式存储业务数据的识别结果，其中，键值(Key)为：待监控数据的时间戳和五元组，值(Value)为所述待监控数据的识别结果和网络传输信息，如待监控数据的基本应用类型、流量等数据。在数据监控模块识别出待识别数据包的五元组和基本应用类型后，直接将识别结果和识别结果的统计数据提交到Redis数据库集群，方便、快捷。采用键值对的方式存储待识别数据包的识别结果，并且用待识别数据包的时间戳和五元组作为Key，用待识别数据包的识别结果作为Value，便于数据监控模块进行快速存储。

[0102] 上述步骤440的具体实施方式参见实施例一的数据处理模块。

[0103] 为了便于对缓存的数据进行，进行分布式存储和分析，如图5所示，在步骤430之后，所述方法进一步包括步骤450：对缓存的所述识别结果和网络传输信息进行格式转换并转发。

[0104] 上述步骤440接收转换后的所述识别结果和网络传输信息后，进行分布式存储和分析，生成监控数据。

[0105] 本发明实施例通过按照同宿同源的规则将待监控的海量数据分发至多个探针服务器，然后，在每个所述探针服务器中创建多个数据监控实例；利用所述数据监控实例根据预设配置采集所述当前探针服务器上的的待监控数据，并进行深度包识别和网络传输信息监控；快速缓存后，发送至大数据平台进行分布式存储和分析，有效地解决了现有技术中DPI技术无法实现海量数据检测的问题，高效地实现了海量数据的监控。

[0106] 在本申请的另一个优选实施例中，所述方法还包括，预先设置多个不同调用优先级的业务类型识别引擎。所述加载业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，进一步包括：按照调用优先级由高到低的顺序依次加载所述业务类型识别引擎识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息。

[0107] 本发明的实施例通过根据业务类型的使用频率，各业务类型识别引擎设置有不同的调用优先级，并按照优先级由高到低的顺序依次调用各业务类型识别引擎，识别所述业务数据的应用类型，以及监测所述应用类型关联的所述业务数据的网络传输信息，可以提

高海量数据的识别效率。

[0108] 本说明书中的各个实施例均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的部分互相参见即可。对于方法实施例而言，由于其与系统实施例基本相似，所以描述的比较简单，相关之处参见系统实施例的部分说明即可。

[0109] 以上对本发明提供的一种基于深度包检测的海量数据监控系统和方法进行了详细介绍，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。

[0110] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件实现。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的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计算机可读存储介质中，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(可以是个人计算机，服务器，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

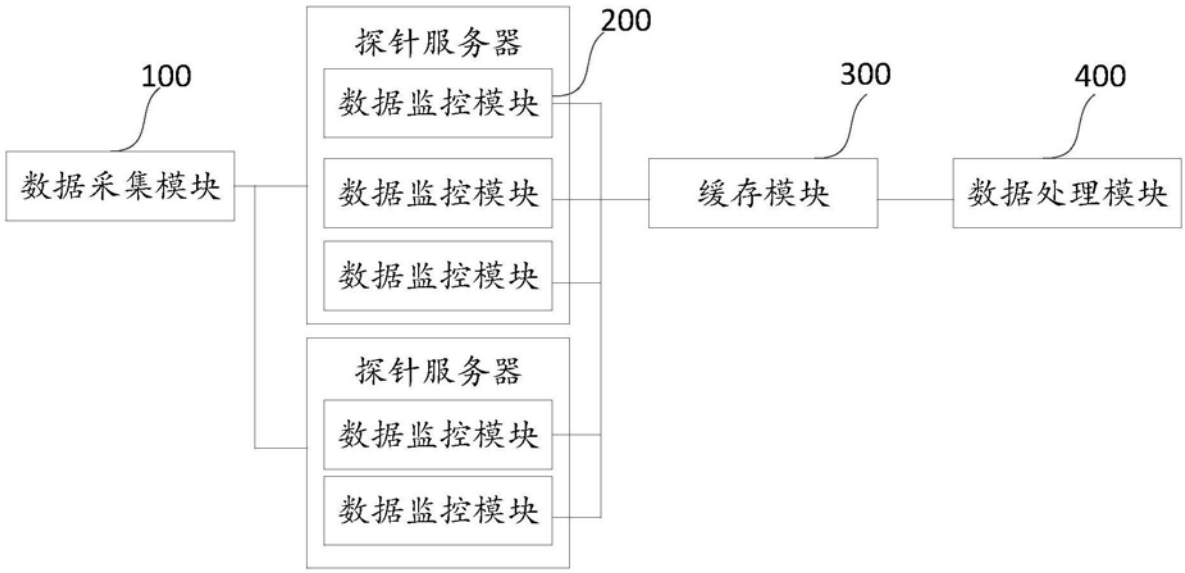

探针服务器
200
100
数据监控模块
300
400
数据采集模块
数据监控模块
缓存模块
数据处理模块
数据监控模块
探针服务器
数据监控模块
数据监控模块

图1

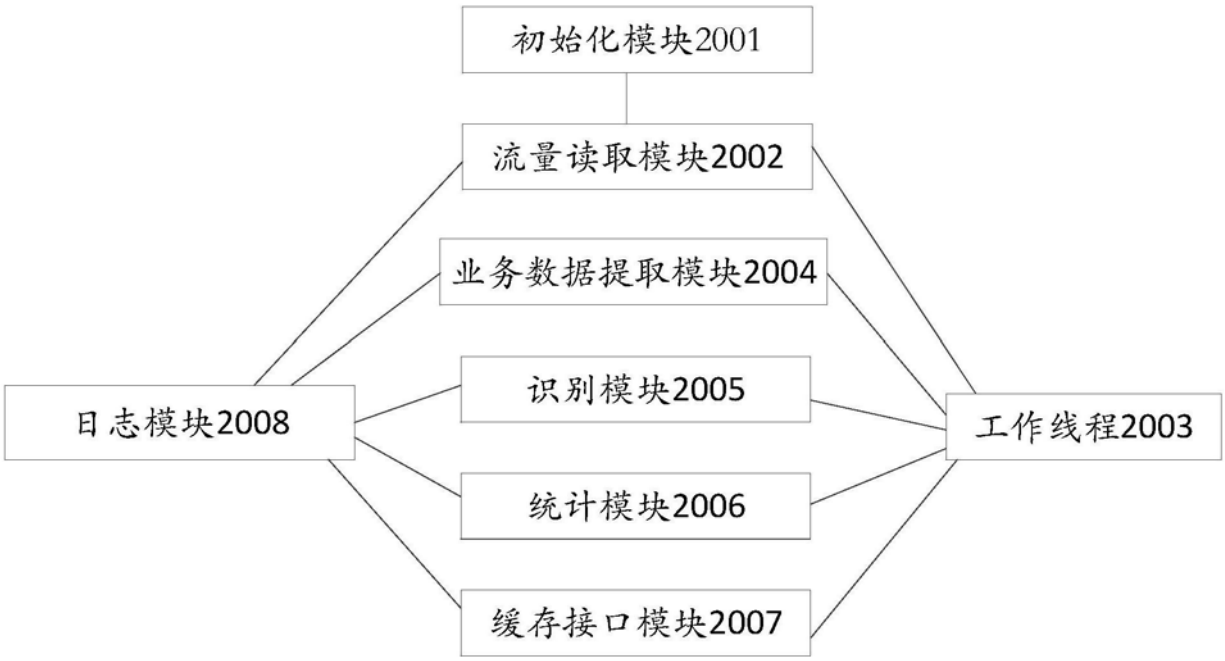

初始化模块2001
流量读取模块2002
业务数据提取模块2004
识别模块2005
日志模块2008
工作线程2003
统计模块2006
缓存接口模块2007

图2

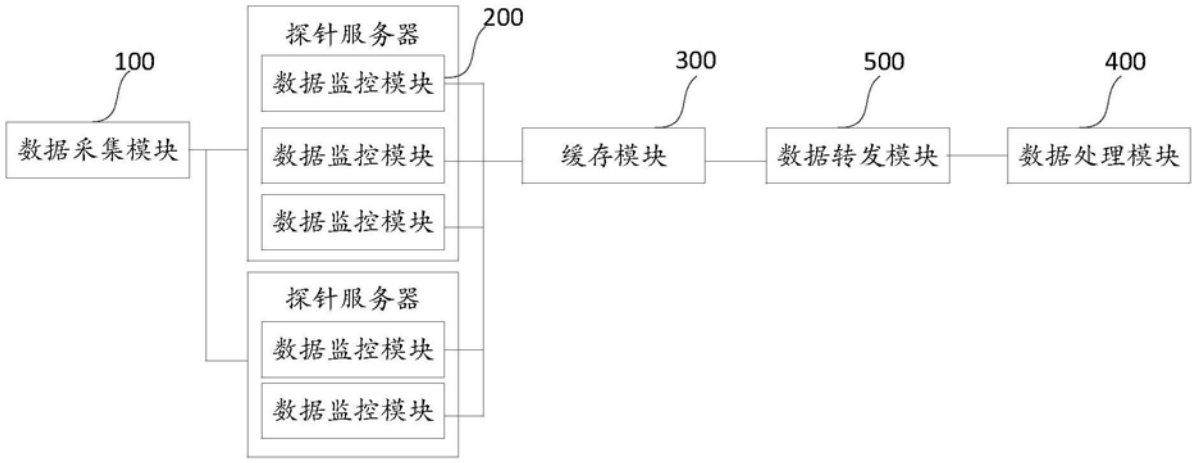

100
数据采集模块
探针服务器
200
数据监控模块
数据监控模块
数据监控模块
探针服务器
数据监控模块
数据监控模块
300
缓存模块
500
数据转发模块
400
数据处理模块

图3

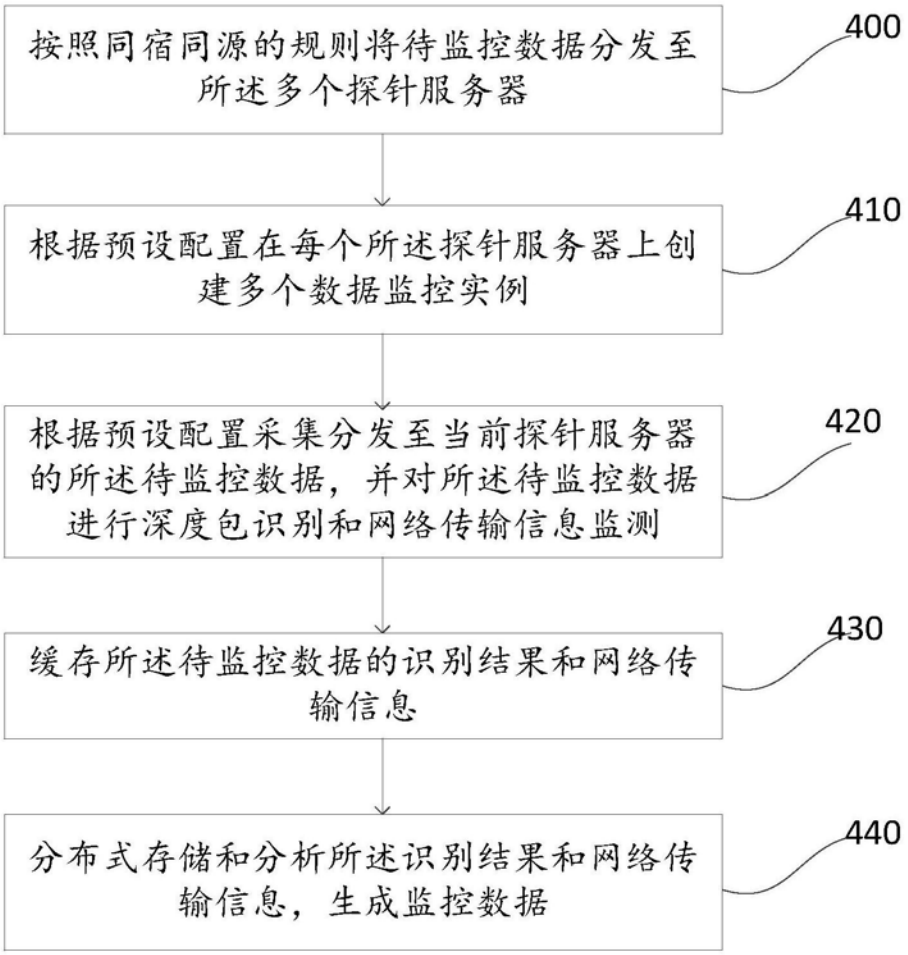

按照同宿同源的规则将待监控数据分发至所述多个探针服务器
400
根据预设配置在每个所述探针服务器上创建多个数据监控实例
410
根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测
420
缓存所述待监控数据的识别结果和网络传输信息
430
分布式存储和分析所述识别结果和网络传输信息，生成监控数据
440

图4

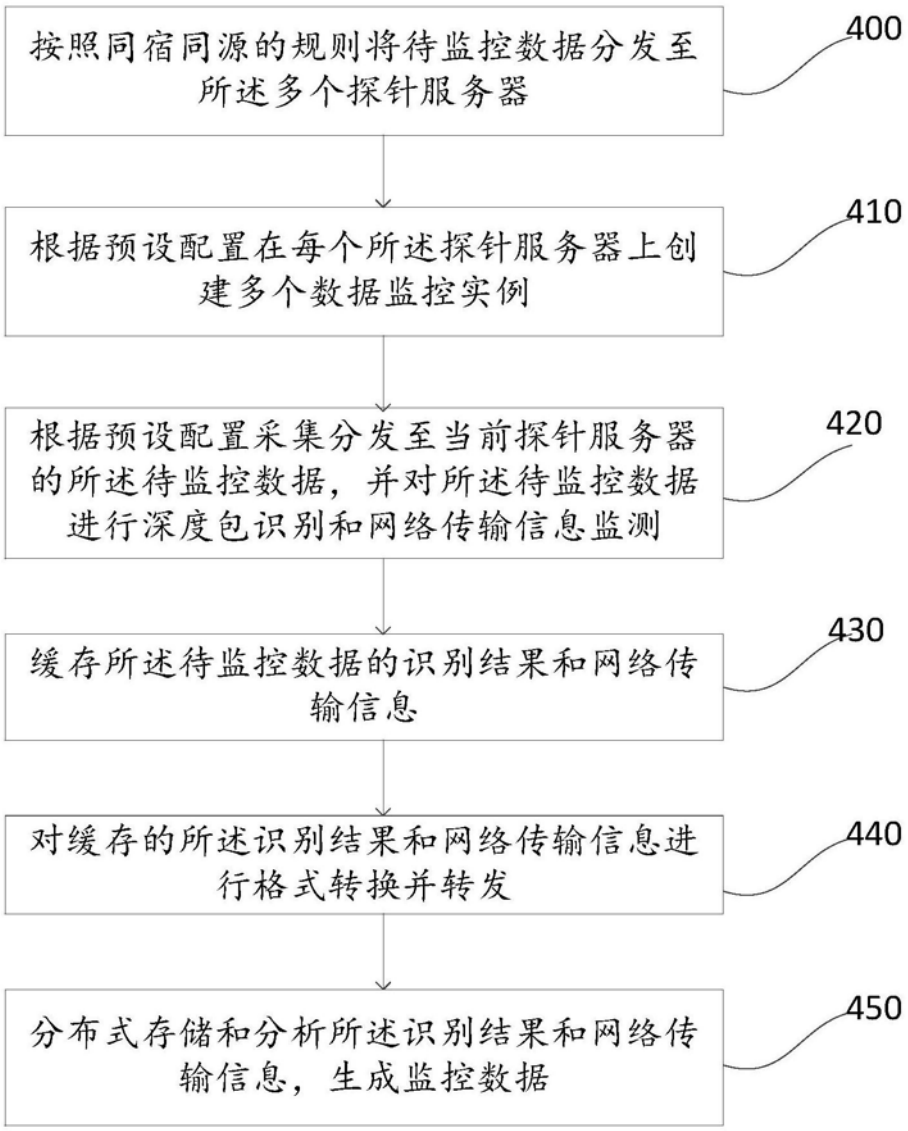

按照同宿同源的规则将待监控数据分发至所述多个探针服务器
400
根据预设配置在每个所述探针服务器上创建多个数据监控实例
410
根据预设配置采集分发至当前探针服务器的所述待监控数据，并对所述待监控数据进行深度包识别和网络传输信息监测
420
缓存所述待监控数据的识别结果和网络传输信息
430
对缓存的所述识别结果和网络传输信息进行格式转换并转发
440
分布式存储和分析所述识别结果和网络传输信息，生成监控数据
450

图5