



1. 一种流量数据包的审计装置,其特征在于,用于监控平台,所述装置包括:

第一接收模块,用于接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

主机定位模块,用于根据所述地址信息确定所述流量数据包对应的主机;

第一发送模块,发送第一指令至所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

第二接收模块,用于接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息;

存储模块,用于将所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型;

第四接收模块,用于获取主机发送的网络流量日志和/或系统应用日志,并触发所述存储模块基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常;

审计模块,基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,

若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。

2. 根据权利要求1所述的流量数据包的审计装置,其特征在于,所述装置还包括:

流量匹配模块,用于根据所述地址信息,以及网络配置信息,判断所述流量数据包的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备;

第二发送模块,用于当所述流量匹配模块判断所述流量数据包的源地址对应的源设备是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是NAT设备时,发送第二指令至NAT设备,所述第二指令用于触发所述NAT设备查询流量数据包翻译前后的地址信息对应关系;

第三接收模块,用于根据所接收的来自NAT设备的流量数据包翻译前后地址信息的对应关系,确定翻译前流量数据包的特征信息,并触发所述主机定位模块以确定所述流量数据包对应的主机。

3. 根据权利要求2所述的流量数据包的审计装置,其特征在于,所述存储模块还用于构建并保存第一主机设备列表,所述第一主机设备列表中的主机安装有所述代理程序;

当所述第二接收模块获取所述第一主机设备列表中主机的主机进程,或所述可执行文件的相关信息,或所述动态链接库的相关信息失败时,所述审计模块判定所述流量数据包

对应的主机通讯异常,对所述流量数据包对应的主机进行通讯管控。

4. 根据权利要求2所述的流量数据包的审计装置,其特征在于,所述装置还包括:

所述存储模块,还用于构建并保存第二主机设备列表,所述第二主机设备列表中的主机未安装所述代理程序;

特征标记模块,用于当判定所述流量数据包的主机在所述第二主机设备列表时,对所述流量数据包进行特征标注,所述特征标注用于表示所述流量数据包是特定设备使用的通讯流量,以用于监测分析所述流量数据包的以下信息中的一种或多种:数量、频度、数据载荷。

5. 一种流量数据包的审计装置,其特征在于,用于网络侧节点,所述装置包括:

第一接收模块,用于接收各个主机发送的流量数据包;

第一解析模块,用于从所述流量数据包中获取用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

第一发送模块,用于向监控平台发送所述流量数据包的特征信息,所述特征信息用于触发所述监控平台根据所述地址信息确定所述流量数据包对应的主机并下发第一指令到所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,使所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型;

所述装置向所述监控平台转发所述主机发送的网络流量日志和/或系统应用日志,触发所述监控平台基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常,基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计,若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常;

其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定。

6. 一种流量数据包的审计装置,其特征在于,用于主机,所述装置包括:

第一发送模块,用于发送流量数据包至网络侧节点,其中,每一个流量数据包中包括用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

第一接收模块,用于接收监控平台发送的第一指令;

信息提取模块,用于根据所述第一指令中的端口信息获取使用流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

第二发送模块,用于发送使用流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息至所述监控平台,触发所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型;

所述主机发送的网络流量日志和/或系统应用日志,并触发所述监控平台基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常;

所述监控平台,基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。

7.一种流量数据包的审计系统,其特征在于,所述系统包括网络侧节点、与所述网络侧节点连接的主机,以及,与所述网络侧节点连接的监控平台;

所述监控平台包括如权利要求1至4任一项所述的流量数据包的审计装置,所述网络侧节点包括如权利要求5所述的流量数据包的审计装置,所述主机包括如权利要求6所述的流量数据包的审计装置。

8.一种流量数据包的审计方法,其特征在于,用于监控平台,所述方法包括以下步骤:

接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

根据所述地址信息确定所述流量数据包对应的主机;

发送第一指令至所述主机,所述第一指令用于触发所述主机根据端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息;

利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型;

获取主机发送的网络流量日志和/或系统应用日志,并基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常;

基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,

若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量

数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。

9.根据权利要求8所述的流量数据包的审计方法,其特征在于,用于监控平台,所述方法还包括以下步骤:

根据所述地址信息,以及网络配置信息,判断所述流量数据包的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备;

确定经NAT设备翻译前后流量数据包的地址信息的对应关系;

确定NAT设备翻译前的流量数据包中包含的特征信息,从而确定NAT设备翻译前的所述流量数据包所对应的主机。

## 流量数据包的审计装置、系统及方法

### 技术领域

[0001] 本发明涉及计算机技术领域,特别涉及一种流量数据包的审计装置、系统及方法。

### 背景技术

[0002] 在传统的流量分析领域,流量分析系统主要采取串接或旁路镜像的方式获取网络通讯数据包,然后对通讯数据包进行分析,完成数据包解析,通讯协议解析,通讯流重组,应用协议解析过程。根据通讯解析的结果,发现可能的异常通讯行为(例如:端口扫描),根据应用层的通讯数据及攻击特征库,判断可能存在的应用层攻击行为。部分产品还会基于流量特征基线,对通讯行为进行进一步的判断。

[0003] 但是,传统的网络流量分析方法,对通讯双方的分析粒度通常只到主机,无法分析到具体是哪个程序,该程序是否可能是非法程序,又是否在近期被更改。这导致了当发现异常情况时,无法判定通讯异常是否确实来自于该主机。当发现异常情况时,无法判定通讯具体是由哪个程序引起。且,现有技术的流量分析方法难以跟踪主机进程在进行版本升级后或其它更改后的通讯特征变化。

### 发明内容

[0004] 针对以上缺陷,本发明提出了一种流量数据包的审计装置、系统及方法,用于解决现有技术的流量分析方法中存在的难以跟踪主机进程在进行版本升级后或其它更改后的通讯特征变化的问题。

[0005] 本申请提供一种流量数据包的审计装置,用于监控平台,所述装置包括:

[0006] 第一接收模块,用于接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

[0007] 主机定位模块,用于根据所述地址信息确定所述流量数据包对应的主机;

[0008] 第一发送模块,发送第一指令至所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

[0009] 第二接收模块,用于接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息;

[0010] 存储模块,用于将所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0011] 进一步的,所述装置还包括:

[0012] 流量匹配模块,用于根据所述地址信息,以及网络配置信息,判断所述流量数据包

的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备；

[0013] 第二发送模块,用于当所述流量匹配模块判断所述流量数据包的源地址对应的源设备是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是NAT设备时,发送第二指令至NAT设备,所述第二指令用于触发所述NAT设备查询流量数据包翻译前后的地址信息对应关系;

[0014] 第三接收模块,用于根据所接收的来自NAT设备的流量数据包翻译前后地址信息的对应关系,确定翻译前流量数据包的特征信息,并触发所述主机定位模块以确定所述流量数据包对应的主机。

[0015] 进一步的,所述装置包括:

[0016] 第四接收模块,用于获取主机发送的网络流量日志和/或系统应用日志,并触发所述存储模块基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常;

[0017] 审计模块,基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,

[0018] 若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

[0019] 若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。

[0020] 进一步的,所述存储模块还用于构建并保存第一主机设备列表,所述第一主机设备列表中的主机安装有所述代理程序;

[0021] 当所述第二接收模块获取所述第一主机设备列表中主机的主机进程,或所述可执行文件的相关信息,或所述动态链接库的相关信息失败时,所述审计模块判定所述流量数据包对应的主机通讯异常,对所述流量数据包对应的主机进行通讯管控。

[0022] 进一步的,所述装置还包括:

[0023] 所述存储模块,还用于构建并保存第二主机设备列表,所述第二主机设备列表中的主机未安装所述代理程序;

[0024] 特征标记模块,用于当判定所述流量数据包的主机在所述第二主机设备列表时,对所述流量数据包进行特征标注,所述特征标注用于表示所述流量数据包是特定设备使用的通讯流量,以用于监测分析所述流量数据包的以下信息中的一种或多种:数量、频度、数据载荷。

[0025] 本申请还提供一种流量数据包的审计装置,用于网络侧节点,所述装置包括:

[0026] 第一接收模块,用于接收各个主机发送的流量数据包;

[0027] 第一解析模块,用于从所述流量数据包中获取用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

[0028] 第一发送模块,用于向监控平台发送所述流量数据包的特征信息,所述特征信息用于触发所述监控平台根据所述地址信息确定所述流量数据包对应的主机并下发第一指令到所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用

所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,使所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型;

[0029] 其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定。

[0030] 本申请还提供一种流量数据包的审计装置,用于主机,所述装置包括:

[0031] 第一发送模块,用于发送流量数据包至网络侧节点,其中,每一个流量数据包中包括用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

[0032] 第一接收模块,用于接收监控平台发送的第一指令;

[0033] 信息提取模块,用于根据所述第一指令中的端口信息获取使用流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

[0034] 第二发送模块,用于发送使用流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息至所述监控平台,触发所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0035] 本申请还提供一种流量数据包的审计系统,所述系统包括网络侧节点、与所述网络侧节点连接的主机,以及,与所述网络侧节点连接的监控平台;

[0036] 所述监控平台包括如上任一所述的流量数据包的审计装置,所述网络侧节点包括如上所述的流量数据包的审计装置,所述主机包括如上所述的流量数据包的审计装置。

[0037] 本申请还提供一种流量数据包的审计方法,用于监控平台,所述方法包括以下步骤:

[0038] 接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号;

[0039] 根据所述地址信息确定所述流量数据包对应的主机;

[0040] 发送第一指令至所述主机,所述第一指令用于触发所述主机根据端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

[0041] 接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息;

[0042] 利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。



[0043] 进一步的,用于监控平台,所述方法还包括以下步骤:

[0044] 根据所述地址信息,以及网络配置信息,判断所述流量数据包的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备;

[0045] 确定经NAT设备翻译前后流量数据包的地址信息的对应关系;

[0046] 确定NAT设备翻译前的流量数据包中包含的特征信息,从而确定NAT设备翻译前的所述流量数据包所对应的主机。

[0047] 本申请提供的流量数据包的识别方法及装置通过对流量数据包进行精确到收发流量的主机进程和/或可执行文件的关联,解决现有技术的流量分析方法中存在的难以跟踪主机进程在进行版本升级后或其它更改后的通讯特征变化的问题。

### 附图说明

[0048] 图1为本申请一个实施例提供的流量数据包的审计方法的流程图;

[0049] 图2为本申请再一实施例提供的流量数据包的审计方法的流程图;

[0050] 图3为本申请一个实施例提供的流量数据包的审计装置的结构框架图;

[0051] 图4为本申请再一实施例提供的流量数据包的审计装置的结构框架图;

[0052] 图5为本申请一个实施例提供的流量数据包的审计装置的结构框架图;

[0053] 图6为本申请一个实施例提供的流量数据包的审计装置的结构框架图;

[0054] 图7为本申请一个实施例提供的流量数据包的审计系统的结构框架图。

### 具体实施方式

[0055] 以下将结合附图所示的具体实施方式对本发明进行详细描述,但这些实施方式并不限制本发明,本领域的普通技术人员根据这些实施方式所做出的结构、方法、或功能上的变换均包含在本发明的保护范围内。

[0056] 如图1所示,其示出了本申请一个实施例提供的流量数据包的审计方法的流程图,包括以下步骤:

[0057] S101、接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号。数据包标识为该流量数据包的唯一标识,可以用于指代该流量数据包。

[0058] S102、根据所述地址信息确定所述流量数据包对应的主机;

[0059] S103、发送第一指令至所述主机,所述第一指令用于触发所述主机根据端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定;

[0060] S104、接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息;

[0061] S105、利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态

链接库的对应关系构建流量数据包审计模型。

[0062] 作为一种可选的实现方式,可以通过在网络侧节点部署一台或多台流量分析装置实现获取所述网络侧节点接收的多条流量数据包。所述流量分析装置可以根据所述流量数据包抽象出该流量数据包的特征信息。所述流量数据包的特征信息包括以下信息中的一种或多种:流量数据包的接收时间,源地址,源端口号,目标地址、目标端口号、流量数据包的协议类型,流量数据包的数据包载荷。

[0063] 具体的,例如对于网络中应用最广泛的TCP/UDP通讯流,流量分析装置可以抽象出流量数据包的五元组信息,所述五元组信息包括源IP地址,源端口号,目标IP地址、目标端口号以及流量数据包的协议类型。而对于GOOSE等基于以太网的三层通讯协议,流量分析装置可以抽象出源MAC地址,目标MAC地址以及流量数据包的协议类型。

[0064] 通过流量分析装置抽象出的关于流量数据包的特征信息中,可以根据特征信息中的源地址和/或目标地址确定各流量数据包对应主机。具体的,例如对于TCP/UDP通讯流,流量数据包的五元组信息中包括源IP地址和目标IP地址,根据源IP地址和目标IP地址可以确定使用该流量数据包的主机。

[0065] 作为一种可选的实现方式,当通过所述特征信息确定使用所述流量数据包的主机时,可以通过安装在该主机上的代理程序收集该主机上的各个主机进程的网络通讯信息,以及各个主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息。

[0066] 具体的,例如对于一个源IP地址为某一主机的TCP通讯流,所述代理程序根据所述特征信息中的源端口号确定所述主机中使用所述流量数据包的具体所述主机进程,并使用所述主机的操作系统提供的接口确定所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息。

[0067] 作为一种可选的实现方式,可执行文件的相关信息包括以下信息中的一种或多种:可执行文件的名称,通过哈希算法获得的关于所述可执行文件的特征值,可执行文件的数字签名,可执行文件的版本号信息。所述动态链接库的相关信息包括以下信息中的一种或多种:动态链接库的名称,动态链接库的保存路径。

[0068] 本申请利用流量数据包的数据包标识指代该流量数据包,利用流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0069] 作为一种可选的实现方式,每当网络侧节点接收到流量数据包时,监控平台都可以依照上述流程构建该流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系,并将该对应关系与本申请实施例提供的流量数据包审计模型进行对比分析,并输出分析结果。其中,本申请实施例提供的流量数据包审计模型为本申请提供的装置在历史运行过程中对主机进程、所述主机进程涉及的可执行文件以及动态链接库经过统计分析生成。

[0070] 具体的,例如,可以有如下分析结果:未能在主机上找到该流量数据包所属的进程,则该流量数据包疑似为其他主机所伪造。该流量数据包来自一个以前没有记录过的未知程序,且同时发现了多个来自该程序的流量数据包,则该流量数据包疑似为扫描攻击行为。获得了对应的进程和可执行文件信息,但该流量数据包的特征(数据流大小,内容,通讯

时间,通讯时长等)与之前相同程序的通讯特征完全不一样,疑似被作为跳板使用。获得了对应的进程和可执行文件信息,但该可执行文件和之前的同位置同名文件相比,已经被修改,签名发生了变化或是缺失,疑似被恶意代码感染。获得了对应进程和可执行文件信息,但该数据流的通讯特征(数据流大小,内容,通讯时间,通讯时长等),与其他众多主机上相同的可执行文件的通讯特征完全不同,疑似被作为跳板使用。来自一个无签名或自签名的可执行程序,通讯行为较奇怪,疑似恶意代码。

[0071] 本申请提供的流量数据包的审计方法将流量分析的粒度从主机细化到主机上运行的程序,基于主机进程和该主机进程所涉及的所有可执行文件进行通讯审计,从而实现了及时发现异常的程序通讯。实现跟踪主机进程在进行版本升级或其它更改后的通讯特征变化。实现基于主机进程的通讯情况构建流量基线,发现主机进程自身的通讯异常。

[0072] 在传统的流量数据包分析方法中,由于无法区分主机进程/可执行文件是长期运行还是偶然使用,因而削弱了流量基线的使用价值。作为一种可选的实现方式,本申请将流量分析的粒度从主机细化到主机上运行的程序,并对主机中的主机进程是长期运行还是偶然使用进行区分。

[0073] 具体的,本申请提供的流量数据包的审计方法还包括:

[0074] 获取所述主机的网络流量日志和/或系统应用日志,并基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常。

[0075] 基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,

[0076] 若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

[0077] 若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。对偶发流量进行解析具体可以为对流量数据包进行分析,完成数据包解析、通讯协议解析、通讯流重组、应用协议解析过程。根据对流量数据包的分析结果,发现可能的异常通讯行为(例如:端口扫描),根据应用层的通讯数据及攻击特征库,判断可能存在的应用层攻击行为。

[0078] 对于相同的主机进程,若版本不同,主机进程的通讯特征会出现变化。因此,作为一种可选的实现方式,本申请提供的流量数据包的审计方法还可以对不同主机上相同的主机进程的通讯行为进行关联分析。其中,不同主机上相同的主机进程的版本可以相同或不同。

[0079] 在实际的使用中,可能会存在某些主机设备未安装代理程序或者无法安装代理程序。这些设备通常为专用网络通讯设备、专用工业控制设备等,这些设备处于设备安全问题的考虑,不被允许随意安装代理程序,这意味着无法通过代理程序进一步确认主机中的主机进程、可执行文件的相关信息和动态链接库的相关信息。但是,对于某些安装有代理程序的主机,如果出现通讯异常的情形同样有可能出现无法通过代理程序进一步确认主机中的主机进程、可执行文件的相关信息和动态链接库的相关信息的问题。因此,需要对安装有代理程序的主机和未安装代理程序的主机进行区分。

[0080] 作为一种可选的实现方式,本申请提供的流量数据包的审计方法还包括构建第一主机设备列表。所述第一主机设备列表中的主机安装有所述代理程序。

[0081] 当所述第一主机设备列表中的主机无法通过所述代理程序获取所述主机进程,或所述可执行文件的相关信息,或所述动态链接库的相关信息时,判定所述流量数据包对应的主机通讯异常,对所述流量数据包对应的主机进行通讯管控。

[0082] 具体的,根据流量数据包的特征信息中的源地址和\或目标地址可以确定使用该流量数据包的主机,检测所述源地址和\或目标地址指向的主机是否存在于第一主机设备列表中。若存在,则进一步判断是否能够通过代理程序通过所述代理程序获取所述主机进程,或所述可执行文件的相关信息,或所述动态链接库的相关信息。若获取失败,则判定所述流量数据包对应的主机通讯异常,对所述流量数据包对应的主机进行通讯管控。

[0083] 作为一种可选的实现方式,本申请提供的流量数据包的检测方法还包括构建第二主机设备列表,所述第二主机设备列表中的主机未安装所述代理程序。

[0084] 当使用所述流量数据包的主机处于所述第二主机设备列表中时,对所述流量数据包进行进一步的特征标注,所述特征标注用于表示所述流量数据包是特定设备使用的通讯流量,例如,特定设备可以是专用网络通讯设备、专用工业控制设备等使用的通讯流量。由于无法通过代理程序获取主机中主机进程的信息,因此,本申请对于第二主机设备列表中的主机进行流量审计时,监测分析所述流量数据包的以下信息中的一种或多种:数量、频度、数据载荷等项目。

[0085] 作为一种可选的实现方式,对于一些难以与具体程序相关联的,为网络通讯提供基础支持的数据包,例如地址解析协议ARP,生成树协议STP等,可以按照传统的流量数据包识别方法,根据通讯数据包的数量、频度、内容等进行监测分析。

[0086] 网络地址翻译(Network Address Translation,NAT)技术是IPv4(Internet Protocol version 4)场景下为了解决IP地址不足和内网安全防护的常见手段。通常分为网络源地址翻译(Source NAT,SNAT)和网络目的地址翻译(Destination NAT,DNAT)。

[0087] 在SNAT场景下,一个内网IP地址访问Internet上的IP地址的网包,在NAT设备上会将其源地址转换为NAT设备自身的公网地址。在DNAT场景下,一个Internet上的IP地址访问NAT设备上的公网地址的网包,在NAT设备上会将其目的地址转换为内网中的某个IP地址。在SNAT场景下,多个内网IP地址可能转换为一个或多个NAT设备上的公网IP地址。在DNAT场景下一个或多个NAT设备上的公网IP地址可能转换为多个内网IP地址。

[0088] 由于网络侧节点接收的流量数据包可能存在IP地址的转换,因此,通过流量分析装置从流量数据包中抽象出的源地址和/或目标地址可能无法直接查找到某一具体的主机。

[0089] 因此,如图2所示,其示出了本申请另一个实施例提供的流量数据包的审计方法的流程图,包括以下步骤:

[0090] S201、接收网络侧节点发送的用以表征流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号。

[0091] S202、根据所述地址信息,以及网络配置信息,判断所述流量数据包的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备,确定经NAT设备翻译前后流量数据的地址信息的对应关系,确定NAT设备翻译前的流量数据包中包含的特征信息,从而确定NAT设备翻译前的所述流量数据包所对应的主机。

[0092] S203、发送第一指令至所述主机,所述第一指令用于触发所述主机根据端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定。

[0093] S204、接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息。

[0094] S205、利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0095] 如步骤S202所述,当流量数据包的源地址来自NAT设备和/或目标地址去往NAT设备时,需要确定NAT设备翻译前后所述流量数据包的对应关系,即,抓取到的SNAT后流量对应哪个内网IP、抓取到的DNAT前流量对应哪个内网 IP。

[0096] 作为一种可选的实现方式,对于DNAT场景,由于Internet上的一个源IP地址、源端口号的请求在经过NAT设备翻译目的IP地址、目标端口号以后,源IP地址、源端口号不会改变,因此通过过滤拥有同样源IP地址、源端口号的NAT设备下行流量即可确定翻译后的目标IP地址和目标端口号,可以直接实现准确的前后流量关联关系计算。

[0097] 但是在SNAT场景下,Internet上的某个公网IP地址可能同时有多个内网IP在对它进行访问,由于SNAT设备会改变源IP和源Port,无法从流量五元组层面精确定SNAT设备前后流量的对应关系。

[0098] 作为另一种可选的实现方式,可以通过使用获取NAT设备的地址转换表的方法确定流量对应关系,例如获取Linux Netfilter实现的NAT设备的Connection tracking表。

[0099] 在确定NAT设备翻译前后的流量数据包的对应关系后,即可获取NAT设备翻译前的流量数据包中包含的特征信息,从而确定NAT设备翻译前的所述流量数据包与所述主机进程、所述可执行文件以及所述动态链接库的对应关系。

[0100] 构建NAT设备翻译前的所述流量数据包与所述主机进程、所述可执行文件以及所述动态链接库的对应关系。

[0101] 传统的网络流量分析方法存在只基于通讯协议的源和/或目标地址信息对数据包的来源及目标进行判断,无法确认源和/或目标地址的真实性的问题。与传统的网络流量分析方法相比,本申请提供的流量数据包的识别方法通过综合在NAT设备上获得的地址转换映射情况,并在主机上安装代理程序,通过代理程序收集主机中各个主机进程的网络通讯状况以及该主机进程所涉及的所有可执行文件的相关信息、主机进程所调用的动态链接库的相关信息。本申请提供的流量数据包的识别方法及装置将网络侧节点接收的多条流量数据包与主机上的各个主机进程进行逐一匹配关联,将流量分析的粒度从主机细化到主机上运行的程序。实现了发现可能的伪造通讯源的流量数据包,并辅助定位攻击源,更精确的判断威胁流量的来源的功能。

[0102] 如图3所示,其示出了本申请一个实施例提供的流量数据包的审计装置的结构框架图,该流量数据包的审计装置可用于监控平台,所述装置包括:第一接收模块301、主机定位模块302、第一发送模块303、第二接收模块304、存储模块305。

[0103] 其中,第一接收模块301,用于接收网络侧节点发送的用以表征流量数据包的特征

信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号。

[0104] 主机定位模块302,用于根据所述地址信息确定所述流量数据包对应的主机。

[0105] 第一发送模块303,发送第一指令至所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定。

[0106] 第二接收模块304,用于接收所述主机发送的使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息。

[0107] 存储模块305,用于将所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0108] 如图4所示,其示出了本申请再一实施例提供的流量数据包的审计装置的结构框架图,该流量数据包的审计装置可用于监控平台。本申请提供的流量数据包的审计装置还包括:审计模块306、流量匹配模块307、第二发送模块308以及第三接收模块309。

[0109] 其中,流量匹配模块307,用于根据所述地址信息,以及网络配置信息,判断所述流量数据包的源地址对应的源设备是否是NAT设备和/或判断所述流量数据包的目标地址对应的目标设备是否是NAT设备。

[0110] 第二发送模块308,用于发送第二指令至NAT设备,所述第二指令用于触发所述NAT设备查询流量数据包翻译前后的地址信息对应关系。

[0111] 第三接收模块309,用于根据所接收的来自NAT设备的流量数据包翻译前后地址信息的对应关系,确定翻译前流量数据包的特征信息,并触发所述主机定位模块以确定所述流量数据包对应的主机。

[0112] 如图4所示,本申请提供的流量数据包的审计装置还包括:第四接收模块310。

[0113] 第四接收模块310,用于获取主机发送的网络流量日志和/或系统应用日志,并触发所述存储模块305基于所述网络流量日志和/或系统应用日志构建通讯基线,所述通讯基线用于判定流量数据包是否存在异常;

[0114] 审计模块306,基于所述主机的网络流量日志和/或系统应用日志,判断所述主机进程和/或可执行文件的运行时长是否大于预设阈值,

[0115] 若运行时长大于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为固定特征流量,并基于所述通讯基线对所述固定特征流量进行审计;

[0116] 若运行时长小于所述预设阈值,则判定所述主机进程和/或可执行文件所使用的流量数据包为偶发流量,对所述偶发流量进行解析,判断所述偶发流量是否存在异常。

[0117] 如图4所示,本申请提供的流量数据包的审计装置还包括:特征标记模块311,用于当判定所述流量数据包的主机在所述第二主机设备列表时,对所述流量数据包进行特征标注,所述特征标注用于表示所述流量数据包是特定设备使用的通讯流量,以用于监测分析所述流量数据包的以下信息中的一种或多种:数量、频度、数据载荷。

[0118] 作为一种可选的实现方式,存储模块305还用于构建并保存第一主机设备列表,所

述第一主机设备列表中的主机安装有所述代理程序；

[0119] 当所述第二接收模块304获取所述第一主机设备列表中主机的主机进程,或所述可执行文件的相关信息,或所述动态链接库的相关信息失败时,所述审计模块306判定所述流量数据包对应的主机通讯异常,对所述流量数据包对应的主机进行通讯管控；

[0120] 所述存储模块305还用于构建并保存第二主机设备列表,所述第二主机设备列表中的主机未安装所述代理程序；

[0121] 当所述主机定位模块确定使用所述流量数据包的主机处于所述第二主机设备列表中时,所述特征标记模块311对所述流量数据包进行进一步的特征标注。

[0122] 如图5所示,其示出了本申请一个实施例提供的流量数据包的审计装置的结构框架图,该流量数据包的审计装置可用于网络侧节点,所述装置包括：

[0123] 第一接收模块501,用于接收各个主机发送的流量数据包,其中,每一个流量数据包中包括用以表征该流量数据包的特征信息,所述特征信息包括地址信息和端口信息,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号；

[0124] 第一解析模块502,用于从所述流量数据包中获取用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号；

[0125] 第一发送模块503,用于向监控平台发送所述流量数据包的特征信息,所述特征信息用于触发所述监控平台根据所述地址信息确定所述流量数据包对应的主机并下发第一指令到所述主机,所述第一指令用于触发所述主机根据所述第一指令中的端口信息获取使用所述流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,使所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型,并将新构建的流量数据包审计模型与监控平台中预存的流量数据包审计模型进行对比分析,并输出分析结果；

[0126] 其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定。

[0127] 如图6所示,其示出了本申请一个实施例提供的流量数据包的审计装置的结构框架图,该流量数据包的审计装置可用于主机,所述装置包括：

[0128] 第一发送模块601,用于发送流量数据包至网络侧节点,其中,每一个流量数据包中包括用以表征该流量数据包的特征信息,所述特征信息包括地址信息、端口信息和数据包标识,所述地址信息包括源地址和/或目标地址,所述端口信息包括源端口号和/或目标端口号；

[0129] 第一接收模块602,用于接收监控平台发送的第一指令；

[0130] 信息提取模块603,用于根据所述第一指令中的端口信息获取使用流量数据包的主机进程、所述主机进程所涉及的所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息,其中,所述主机进程为所述主机安装的代理程序根据所述端口信息确定,所述可执行文件的相关信息以及动态链接库的相关信息为所述代理程序根据所述主机进程确定；

[0131] 第二发送模块604,用于发送使用流量数据包的主机进程、所述主机进程所涉及的

所有可执行文件的相关信息,以及,所述主机进程使用的动态链接库的相关信息至所述监控平台,触发所述监控平台利用所述流量数据包的数据包标识分别与主机进程、可执行文件以及动态链接库的对应关系构建流量数据包审计模型。

[0132] 如图7所示,其示出了本申请一个实施例提供的流量数据包的审计系统的结构框架图,该流量数据包的审计系统包括:如上所述的网络侧节点701、与所述网络侧节点连接的主机702,以及,与所述网络侧节点连接的监控平台703。

[0133] 综上所述,本申请提供的流量数据包的审计装置、系统及方法通过综合在NAT设备上获得的地址转换映射情况,并在主机上安装代理程序,通过代理程序收集主机中各个主机进程的网络通讯状况以及该主机进程所涉及的所有可执行文件的相关信息、主机进程所调用的动态链接库的相关信息。本申请提供的流量数据包的识别方法及装置将网络侧节点接收的多条流量数据包与主机上的各个主机进程进行逐一匹配关联,本申请将流量分析的粒度从主机细化到主机上运行的程序。

[0134] 以上所揭露的仅为本发明的较佳实施例而已,然其并非用以限定本发明之权利范围,本领域普通技术人员可以理解:在不脱离本发明及所附的权利要求的精神和范围内,改变、修饰、替代、组合、简化,均应为等效的置换方式,仍属于发明所涵盖的范围。



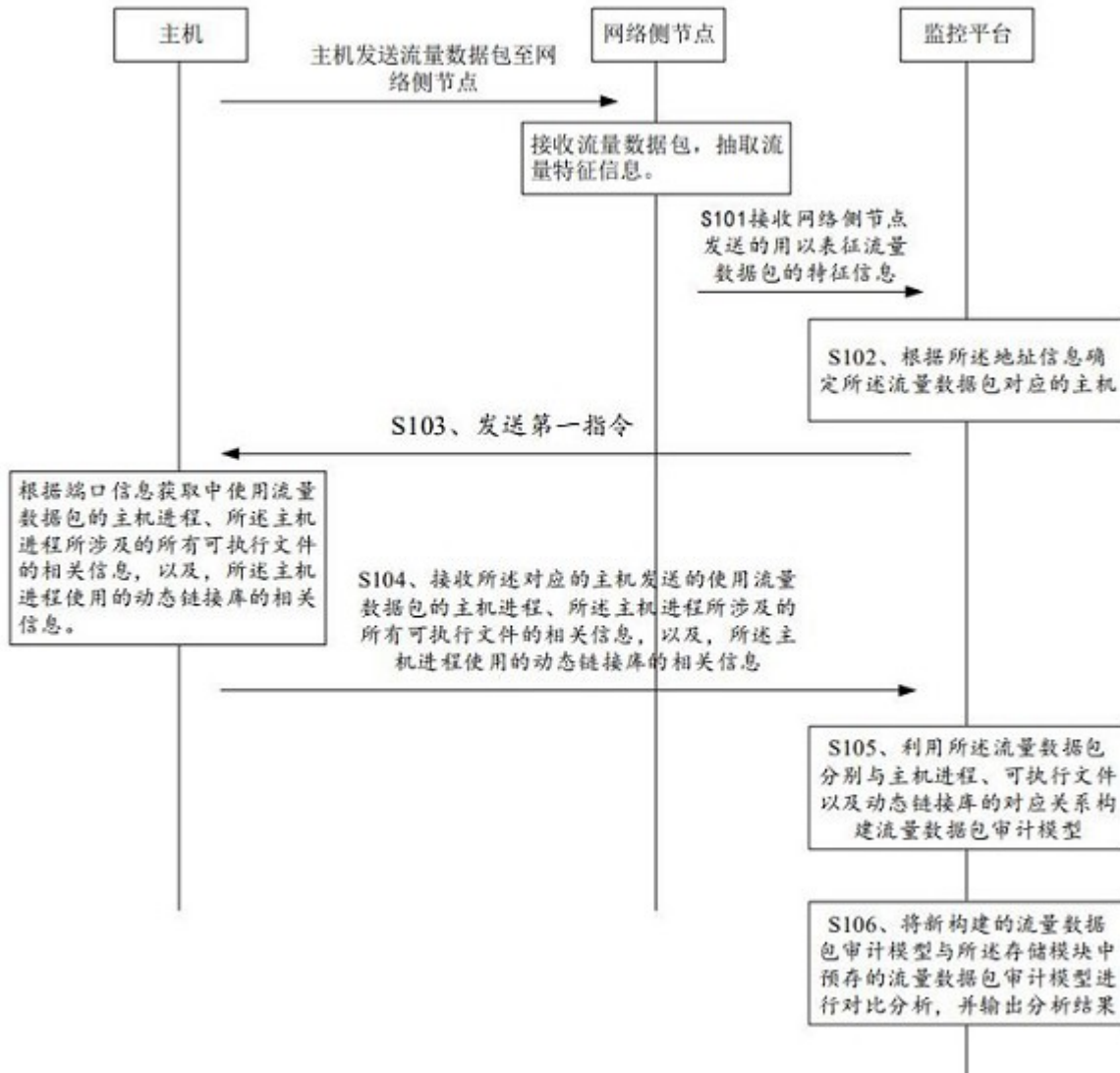


图1

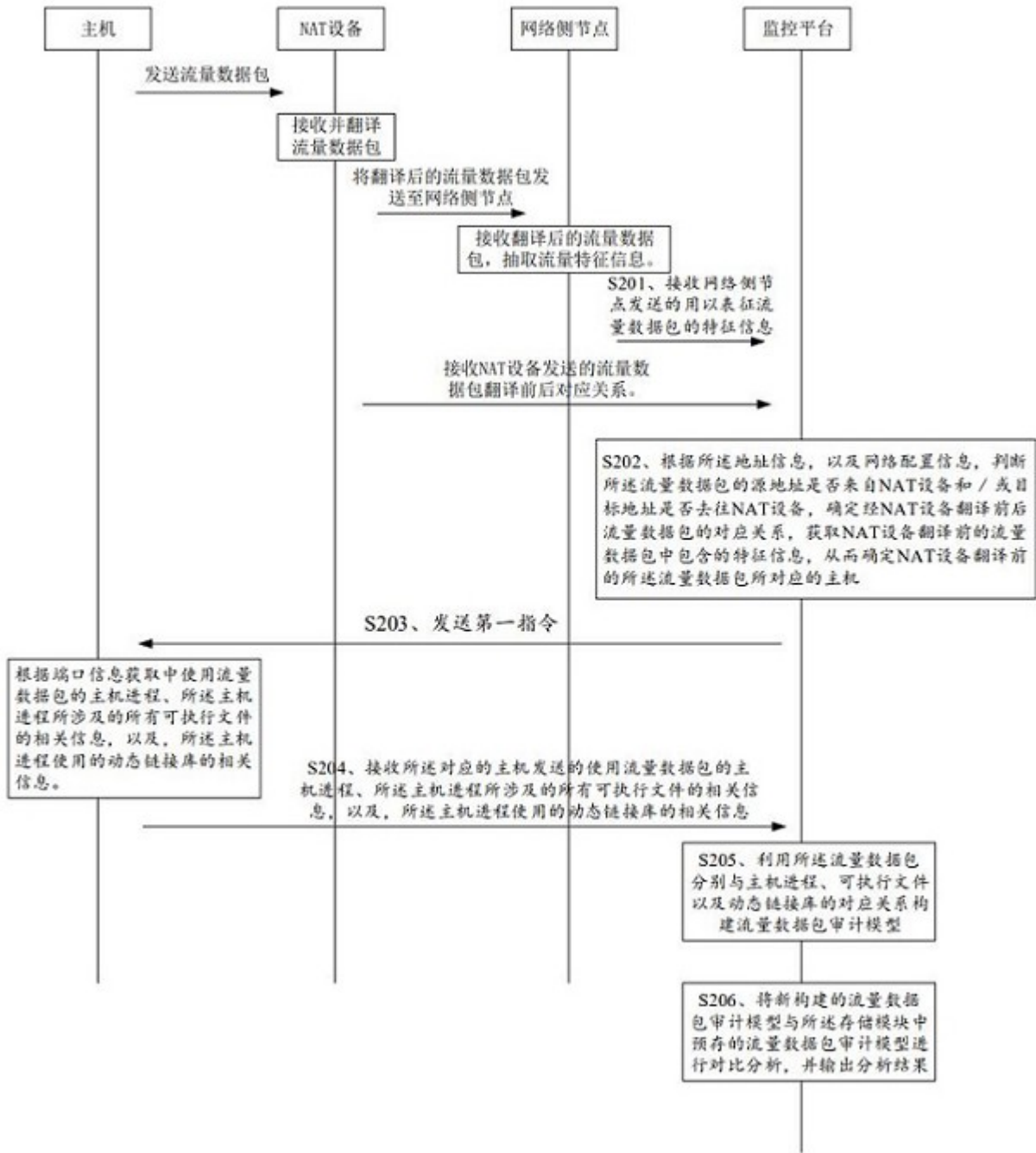


图2

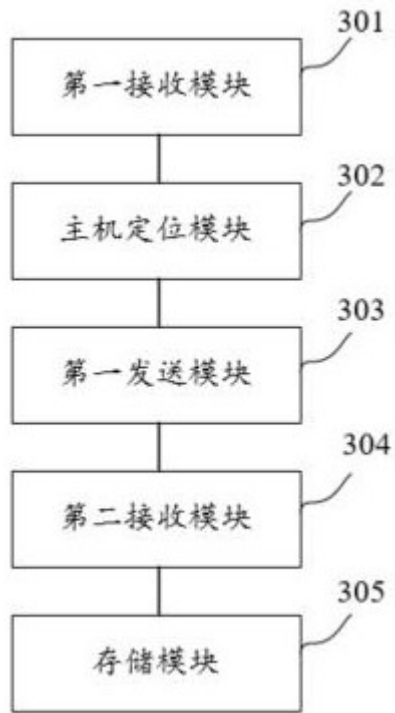


图3

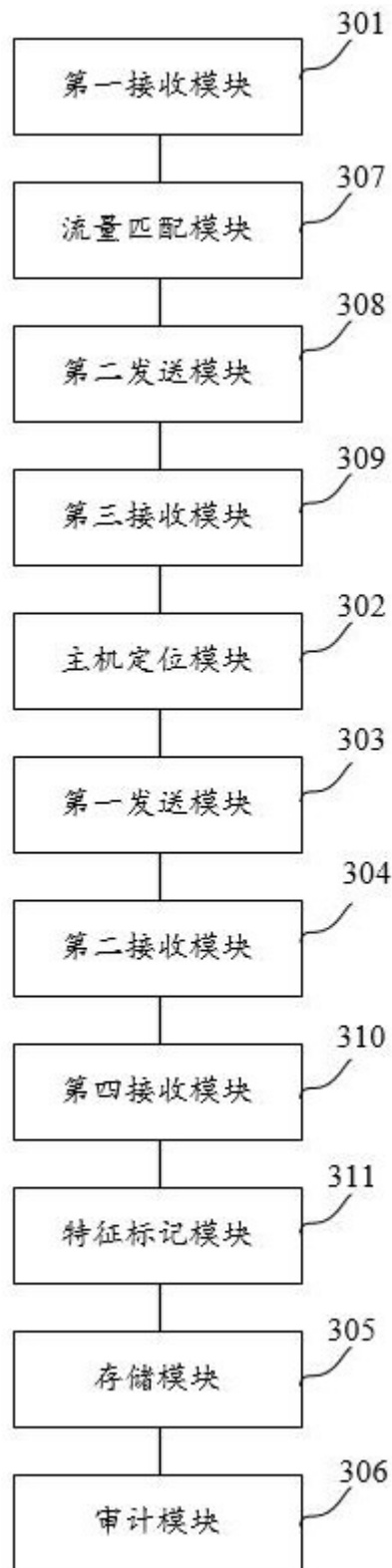


图4

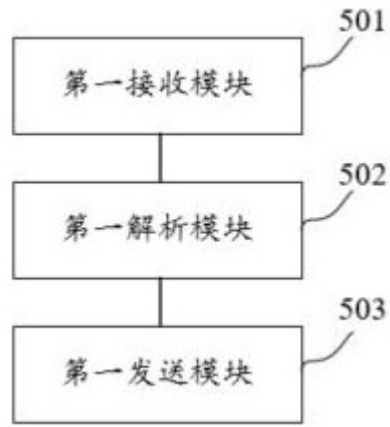


图5

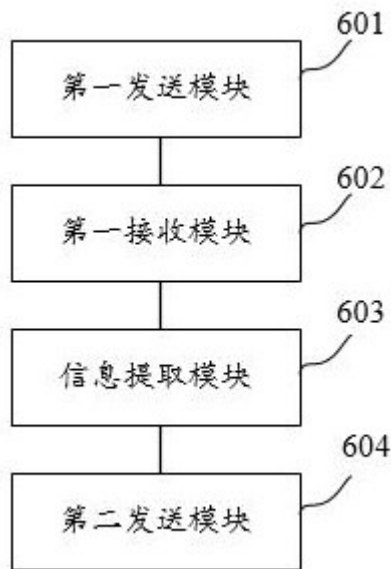


图6

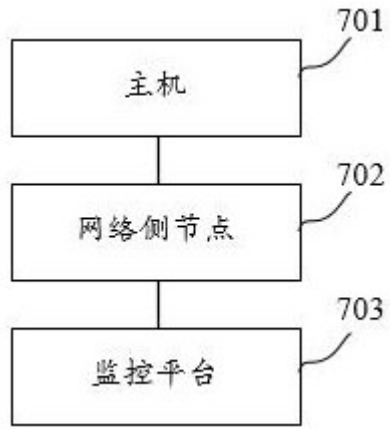


图7