



(12) 发明专利申请

(10) 申请公布号 CN 114697068 A

(43) 申请公布日 2022. 07. 01

(21) 申请号 202111573232.2

H04L 67/02 (2022.01)

(22) 申请日 2021.12.21

(66) 本国优先权数据

202011639885.1 2020.12.31 CN

(71) 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

申请人 清华大学

(72) 发明人 万荣飞 朱安南 张甲 段海新

(74) 专利代理机构 广州三环专利商标代理有限公司 44202

专利代理师 石朝清

(51) Int. Cl.

H04L 9/40 (2022.01)

H04L 41/0631 (2022.01)

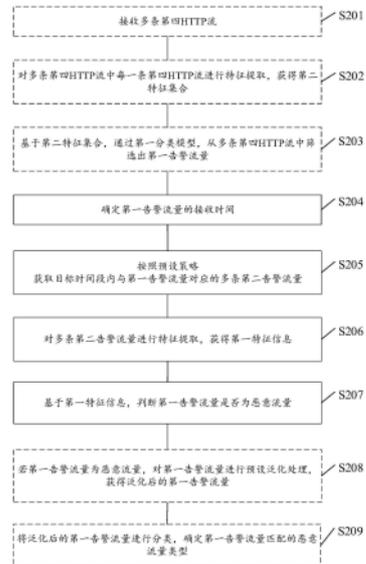
权利要求书4页 说明书21页 附图9页

(54) 发明名称

一种恶意流量识别方法及相关装置

(57) 摘要

本申请实施例提供了一种恶意流量识别方法及相关装置,其中,一种恶意流量识别方法,可包括:确定第一告警流量的接收时间;基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;对所述多条第二告警流量进行特征提取,获得第一特征信息;基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。实施本申请实施例,可以通过多流回溯的方法提升现网中恶意流量识别的准确率。



1. 一种恶意流量识别方法,其特征在于,包括:

确定第一告警流量的接收时间;

基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;

对所述多条第二告警流量进行特征提取,获得第一特征信息;

基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

2. 根据权利要求1所述方法,其特征在于,所述预设策略包括:第一策略、第二策略、第三策略中的一个或多个,其中,所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略;所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略;所述第三策略为基于所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。

3. 根据权利要求2所述方法,其特征在于,所述预设策略为所述第一策略;所述基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:

获取所述第一告警流量的IP地址和UA信息;

采集在所述目标时间段内所述IP地址发送的多条HTTP流中,与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。

4. 根据权利要求2所述方法,其特征在于,所述预设策略为所述第二策略,所述基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:

获取所述第一告警流量的所述IP地址;

采集在所述目标时间段内所述IP地址发送的多条第一HTTP流;

对多条第一HTTP流按照所述预设泛化规则进行泛化处理,获得多条第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;

从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于所述预设阈值的第二HTTP流为所述第二告警流量。

5. 根据权利要求2所述方法,其特征在于,所述预设策略为所述第三策略,所述基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:

获取所述第一告警流量的所述IP地址和所述HTTP Header信息;

采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;

分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;

对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;

基于所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。

6. 根据权利要求1-5所述任意一项方法,其特征在于,所述第一特征信息为特征表示向

量;所述对所述多条第二告警流量进行特征提取,获得第一特征信息,包括:

对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;

根据所述行为特征信息,获取所述特征表示向量。

7.根据权利要求1-6所述任意一项方法,其特征在于,所述根据所述第一特征信息,判断所述第一告警流量是否为恶意流量,包括:

基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;

基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;

基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。

8.根据权利要求1-7所述任意一项方法,其特征在于,所述方法还包括:

若所述第一告警流量为恶意流量,对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量;

将所述泛化后的第一告警流量进行分类,确定所述第一告警流量匹配的恶意流量类型。

9.根据权利要求1所述方法,其特征在于,所述确定第一告警流量的接收时间之前,还包括:

接收多条第四HTTP流;

对所述多条第四HTTP流中每一条第四HTTP流进行特征提取,获得第二特征集合,所述第二特征集合包括所述多条第四HTTP流分别对应的第二特征信息;

基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。

10.根据权利要求9所述方法,其特征在于,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。

11.一种恶意流量识别装置,其特征在于,包括:

确定单元,用于确定第一告警流量的接收时间;

回溯单元,用于基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;

提取单元,用于对所述多条第二告警流量进行特征提取,获得第一特征信息;

判断单元,用于基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

12.根据权利要求11所述装置,其特征在于,所述预设策略包括:第一策略、第二策略、第三策略中的一个或多个,其中,所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略;所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略;所述第三策略为基于

所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。

13. 根据权利要求12所述装置,其特征在于,所述预设策略为所述第一策略;所述回溯单元,具体用于:

获取所述第一告警流量的IP地址和UA信息;

采集在所述目标时间段内所述IP地址发送的多条HTTP流中,与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。

14. 根据权利要求12所述装置,其特征在于,所述预设策略为所述第二策略,所述回溯单元,具体用于:

获取所述第一告警流量的所述IP地址;

采集在所述目标时间段内所述IP地址发送的多条第一HTTP流;

对多条第一HTTP流按照所述预设泛化规则进行泛化处理,获得多条第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;

从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于预设阈值的目标第二HTTP流为所述第二告警流量。

15. 根据权利要求12所述装置,其特征在于,所述预设策略为所述第三策略,所述回溯单元,具体用于:

获取所述第一告警流量的所述IP地址和所述HTTP Header信息;

采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;

分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;

对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;

基于所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。

16. 根据权利要求11-15所述任意一项装置,其特征在于,所述第一特征信息为特征表示向量;所述提取单元,具体用于:

对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;

根据所述行为特征信息,获取所述特征表示向量。

17. 根据权利要求11-16所述任意一项装置,其特征在于,所述判断单元,具体用于:

基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;

基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;

基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。

18. 根据权利要求11-17所述任意一项装置,其特征在于,所述装置还包括:

泛化单元,用于若所述第一告警流量为恶意流量,对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量;

分类单元,用于将所述泛化后的第一告警流量进行分类,确定所述第一告警流量匹配的恶意流量类型。

19. 根据权利要求11所述装置,其特征在于,所述装置还包括告警流量单元,所述告警流量单元,用于:

确定第一告警流量的接收时间之前,接收多条第四HTTP流;

对所述多条第四HTTP流中每一条第四HTTP流进行特征提取,获得第二特征集合,所述第二特征集合包括所述多条第四HTTP流分别对应的第二特征信息;

基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。

20. 根据权利要求19所述装置,其特征在于,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。

21. 一种服务设备,其特征在于,包括处理器和存储器,其中,所述存储器用于存储恶意流量识别程序代码,所述处理器用于调用所述恶意流量识别程序代码来执行权利要求1-10任一项所述的方法。

22. 一种芯片系统,其特征在于,所述芯片系统包括至少一个处理器,存储器和接口电路,所述存储器、所述接口电路和所述至少一个处理器通过线路互联,所述至少一个存储器中存储有指令;所述指令被所述处理器执行时,权利要求1-10中任意一项所述的方法得以实现。

23. 一种计算机可读存储介质,其特征在于,所述计算机存储介质存储有计算机程序,该计算机程序被处理器执行时实现上述权利要求1-10任意一项所述的方法。

24. 一种计算机程序,其特征在于,所述计算机程序包括指令,当所述计算机程序被计算机执行时,使得所述计算机执行如权利要求1-10中任意一项所述的方法。

一种恶意流量识别方法及相关装置

[0001] 本申请要求于2020年12月31日提交中国专利局、申请号为202011639885.1、申请名称为“一种恶意流量识别方法及相关装置”的中国专利申请的优先权,其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及通信技术领域,尤其涉及一种恶意流量识别方法及相关装置。

背景技术

[0003] 超文本传输协议(HyperText Transfer Protocol,HTTP)协议作为目前最重要的协议,在互联网上得到广泛应用。为了方便通信和掩盖恶意行为,各类恶意软件,如木马病毒等的通信手段往往会采用HTTP通信方式,其中,主要是指受控节点与木马的命令与控制服务器(Command and Control Server,CC/C2)之间的通信。由于木马病毒的更新迭代非常迅速,更新迭代后的木马病毒会与之前的通信流量有着较为明显的差异。当前对采用HTTP恶意流量检测思路有两种:1)从流量层来检测,即通过提取流量中的特征进行检测;2)从主机行为来检测,即通过提取受感染的主机行为中的特征进行检测。其中,处理提取好的特征的方法主要有两种:1)基于无监督的聚类检测方法;2)基于有监督模型的检测方法。

[0004] 然而,无论是从流量层对应的特征来检测,还是从主机行为对应的特征来检测,该无监督的聚类检测方法和有监督模型检测方法都仅考虑了单流的特征,即,一条HTTP流的特征,并没有考虑的恶意CC通信的多流网络行为特征,即,多条HTTP流的特征。目前的检测方法,基础信息丰富度不足,无法有效准确的识别流量是否为恶意流量。而且,很多流氓软件的行为与CC流量的特征行为在单流层面上来看是相似的,仅仅使用单流特征分析方法,无法有效的区分流氓软件和恶意软件。

[0005] 因此,如何更加精准检测出现网中的恶意流量,是亟待解决的问题。

发明内容

[0006] 本申请实施例提供一种恶意流量识别方法及相关装置,以提升恶意流量识别的准确率。

[0007] 第一方面,本申请实施例提供了一种恶意流量识别方法,可包括:

[0008] 确定第一告警流量的接收时间;基于预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;对所述多条第二告警流量进行特征提取,获得第一特征信息;基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

[0009] 实施第一方面的实施例,恶意流量识别装置可以从单条流量(即:第一告警流量)的接收时间起,按照预设策略回溯获取与该单条流量匹配的多条流量(即:多条第二告警流量)。然后,对回溯到的多条流量进行特征提取,获得特征信息,使得恶意流量识别装置可以

根据该特征信息对上述单条流量进行分类,从而确定该单条流量是否为恶意流量。其中,该多条第二告警流量与第一告警流量之间的相似度均大于预设阈值。这种根据单条流量相似的多条流量的特征信息对单条流量进行分类的方法,使得恶意流量识别装置对流量进行识别时,可以充分考虑恶意CC通信流量的多流网络行为的特征,从而更加精准的检测并分辨现网中的恶意流量。避免了现有技术检测过程中,由于现网中流量情况相对较为复杂,针对单条HTTP流的检测具备的偶然性。另外,本申请实施例从多流角度对流量的通信行为进行观察,将多个告警流量基于一种或多种的预设策略回溯到不同簇,利用每条告警流所属不同簇的统计其特征信息,根据该特征信息研判正负性(即,告警流量是否为恶意流量),从而杜绝了偶然误差。这种观察恶意流量在一定时间内整体的通信行为,可以从行为角度判断恶意样本,使得最终的多流判断结果更为鲁棒,同时也具备行为上的可解释性。而且,本申请实施例对于多流流量无论是从流量层对应的特征来检测,还是从主机行为对应的特征来检测,基础信息丰富度都足够恶意流量识别装置有效准确的识别流量是否为恶意流量。从而,可以从多流的特征上区分流氓软件的通信流量和恶意软件的通信流量,提高恶意流量识别的准确率。

[0010] 在一种可能实现的方式中,所述目标时间段为以所述接收时间为起点向后预设时长的时间段,或者为以所述接收时间为终点向前预设时长的时间段。在本申请实施例中,可以以接收到第一告警流量的接收时间为端点,向前或向后取预设时长的时间段,以保证获得尽可能多的与第一告警流量相似的多条第二告警流量。

[0011] 在一种可能实现的方式中,所述预设策略包括:第一策略、第二策略、第三策略中的一个或多个,其中,所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略;所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略;所述第三策略为基于所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。实施本申请实施例,多种流量回溯方式均可以精准的回溯到第一告警流量同源的多条流量,从而可以根据该多条流量的行为特征识别出第一告警流量是否为恶意流量,提高了识别恶意流量的精准度。

[0012] 在一种可能实现的方式中,所述预设策略包括所述第一策略;所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的IP地址和UA信息;采集在所述目标时间段内所述IP地址发送的多条HTTP流中,与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。实施本申请实施例,通过回溯第一告警信息同源IP地址和同UA信息的流量,可以回溯到同个软件、同个服务设备或同个应用发送的多条流量,从而根据回溯到的多条流量的行为特征确定第一告警流量是否为恶意流量,提高了识别恶意流量的准确率。

[0013] 在一种可能实现的方式中,所述预设策略包括所述第二策略,所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的所述IP地址;采集在所述目标时间段内所述IP地址发送的多条第一HTTP流;对多条第一HTTP流按照所述预设泛化规则进行泛化处理,获得多条第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于预设阈

值的第二HTTP流为所述第二告警流量。实施本申请实施例,通过泛化后,计算流量之间相似度的方法,进而确定与第一告警流量同簇的(同个软件、不同应用发送的)多条流量(相似度超过预设阈值),进而根据该多条流量的行为特征确定第一告警流量是否为恶意流量,提高了识别恶意流量的准确度。

[0014] 在一种可能实现的方式中,所述预设策略包括所述第三策略,所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的所述IP地址和所述HTTP Header信息;采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;基于所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。实施本申请实施例,通过提取流量中的HTTP Header序列(sequence)信息进行回溯的方法,可以回溯到同个软件中不同应用发送的多条流量,进而根据该多条流量的行为特征确定第一告警流量是否为恶意流量,提高了识别恶意流量的准确度。

[0015] 在一种可能实现的方式中,所述第一特征信息为特征表示向量;所述对所述多条第二告警流量进行特征提取,获得第一特征信息,包括:对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;根据所述行为特征信息,获取所述特征表示向量。实施本申请实施例,对多流流量进行行为特征提取,可以很好的分辨流氓软件对应的流量和恶意软件对应的流量,提高了恶意流量识别的准确度。

[0016] 在一种可能实现的方式中,所述根据所述第一特征信息,判断所述第一告警流量是否为恶意流量,包括:基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。实施本申请实施例,通过综合考虑通过回溯模型进行检测的第一检测结果和通过基线模型进行检测的第二检测结果,最终确定第一告警流量是否为恶意流量,大大提高了恶意流量识别的准确度。

[0017] 在一种可能实现的方式中,所述方法还包括:若所述第一告警流量为恶意流量,对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量;将所述泛化后的第一告警流量进行分类,确定所述第一告警流量匹配的恶意流量类型。实施本申请实施例,通过对泛化处理后的第一告警流量分类,可以确定与第一告警流量匹配的恶意流量类型,以便更好地维护网络安全。

[0018] 在一种可能实现的方式中,所述确定第一告警流量的接收时间之前,还包括:接收多条第四HTTP流;对所述多条第四HTTP流中每一条第四HTTP流按照预设特征提取规则进行特征提取,获得第二特征集合,所述第二特征集合包括:所述多条第四HTTP流分别对应的第二特征信息;基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。实施本申请实施例,通过第一分类模型,根据单流流量特征(如手工特征和/或表示学习特征),从多条第四HTTP流中筛选出疑似恶意流量的第一告警流量(即,单

流过滤),可以有效降低检测过程中对大量无关数据流的存储与检测,提高恶意流量的分析效率。

[0019] 在一种可能实现的方式中,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。实施本申请实施例,在实现单流过滤提取现网流量中疑似恶意流量的第一告警流量时,可以通过识别流量对应的手工特征和/或表示学习特征实现,例如:提取所述多条第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;又例如:基于表示学习模型提取所述多条第四HTTP流对应的高维特征。提高了单流过滤识别疑似恶意流量的第一告警流量的准确度,提高恶意流量的分析效率。

[0020] 第二方面,本申请实施例提供了一种恶意流量识别装置,包括:

[0021] 确定单元,用于确定第一告警流量的接收时间;

[0022] 回溯单元,用于按照预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;

[0023] 提取单元,用于对所述多条第二告警流量进行特征提取,获得第一特征信息;

[0024] 判断单元,用于基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

[0025] 在一种可能实现的方式中,所述预设策略包括:第一策略、第二策略、第三策略中的一个或多个,其中,所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略;所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略;所述第三策略为基于所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。

[0026] 在一种可能实现的方式中,所述预设策略包括所述第一策略;所述回溯单元,具体用于:获取所述第一告警流量的IP地址和UA信息;采集在所述目标时间段内所述IP地址发送的多条HTTP流中,与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。

[0027] 在一种可能实现的方式中,所述预设策略包括所述第二策略,所述回溯单元,具体用于:获取所述第一告警流量的所述IP地址;采集在所述目标时间段内所述IP地址发送的多条第一HTTP流;对多条第一HTTP流按照所述预设泛化规则进行泛化处理,获得多条第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于预设阈值的第二HTTP流为所述第二告警流量。

[0028] 在一种可能实现的方式中,所述预设策略包括所述第三策略,所述回溯单元,具体用于:获取所述第一告警流量的所述IP地址和所述HTTP Header信息;采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;基于

所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。

[0029] 在一种可能实现的方式中,所述第一特征信息为特征表示向量;所述提取单元,具体用于:对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;根据所述行为特征信息,获取所述特征表示向量。

[0030] 在一种可能实现的方式中,所述判断单元,具体用于:基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。

[0031] 在一种可能实现的方式中,所述装置还包括:泛化单元,用于若所述第一告警流量为恶意流量,对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量;分类单元,用于将所述泛化后的第一告警流量进行分类,确定所述第一告警流量匹配的恶意流量类型。

[0032] 在一种可能实现的方式中,所述装置还包括告警流量单元,所述告警流量单元,用于:确定第一告警流量的接收时间之前,接收多条第四HTTP流;对所述多条第四HTTP流中每一条第四HTTP流按照预设特征提取规则进行特征提取,获得第二特征集合,所述第二特征集合包括:所述多条第四HTTP流分别对应的第二特征信息;基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。

[0033] 在一种可能实现的方式中,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。

[0034] 第三方面,本申请实施例提供一种服务设备,该服务设备中包括处理器,处理器被配置为支持该服务设备实现第一方面提供的恶意流量识别方法中相应的功能。该服务设备还可以包括存储器,存储器用于与处理器耦合,其保存该服务设备必要的程序指令和数据。该服务设备还可以包括通信接口,用于该服务设备与其他设备或通信网络通信。

[0035] 第四方面,本申请实施例提供一种计算机可读存储介质,用于储存为上述第二方面提供的一种恶意流量识别装置所用的计算机软件指令,其包含用于执行上述方面所设计的程序。

[0036] 第五方面,本申请实施例提供了一种计算机程序,该计算机程序包括指令,当该计算机程序被计算机执行时,使得计算机可以执行上述第二方面中的恶意流量识别装置所执行的流程。

[0037] 第六方面,本申请提供了一种芯片系统,该芯片系统包括处理器,用于支持终端设备实现上述第一方面中所涉及的功能,例如,生成或处理上述恶意流量识别方法中所涉及的信息。在一种可能的设计中,所述芯片系统还包括存储器,所述存储器,用于保存数据发送设备必要的程序指令和数据。该芯片系统,可以由芯片构成,也可以包含芯片和其他分立器件。

附图说明

[0038] 为了更清楚地说明本申请实施例或背景技术中的技术方案,下面将对本申请实施例或背景技术中所需要使用的附图进行说明。

[0039] 图1是本申请实施例提供了一种恶意流量识别系统构架示意图。

[0040] 图2是本申请实施例提供了一种恶意流量识别方法的流程示意图。

[0041] 图3是本申请实施例提供了一种恶意流量识别的框架示意图。

[0042] 图4是本申请实施例提供了一种特征提取的示意图。

[0043] 图5是本申请实施例提供了一种按照第一策略回溯流量的流程示意图。

[0044] 图6是本申请实施例提供了一种根据第一策略回溯的多条流量示意图。

[0045] 图7是本申请实施例提供了一种按照第二策略回溯流量的流程示意图。

[0046] 图8是本申请实施例提供了一种流量泛化前后的示意图。

[0047] 图9是本申请实施例提供了一种按照第三策略回溯流量的流程示意图。

[0048] 图10是本申请实施例提供了一种获得第一特征信息的方法流程示意图。

[0049] 图11是本申请实施例提供了一种以 E_n 为自变量, a_n 为因变量的函数图像。

[0050] 图12是本申请实施例提供了一种确定恶意流量所属种类的流程示意图。

[0051] 图13是本申请实施例提供了一种恶意流量识别装置的结构示意图。

[0052] 图14是本申请实施例提供的另一种恶意流量识别装置的结构示意图。

具体实施方式

[0053] 下面将结合本申请实施例中的附图,对本申请实施例进行描述。

[0054] 本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象,而不是用于描述特定顺序。此外,术语“包括”和“具有”以及它们任何变形,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、产品或设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0055] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行描述。在本申请中,“至少一个”是指一个或者多个,“多个”是指两个或两个以上。“和/或”,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的情况,其中A,B可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达,是指的这些项中的任意组合,包括单项(个)或复数项(个)的任意组合。例如,a,b或c中的至少一项(个),可以表示:a,b,c,a和b,a和c,b和c或a,b和c,其中a、b和c可以是单个,也可以是多个。

[0056] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0057] 在本说明书中使用的术语“部件”、“模块”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如,部件可以是但不限于,在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示,在计

算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中,部件可位于一个计算机上和/或分布在2个或更多个计算机之间。此外,这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组(例如来自与本地系统、分布式系统和/或网络间的另一部件交互的二个部件的数据,例如通过信号与其它系统交互的互联网)的信号通过本地和/或远程进程来通信。

[0058] 首先,对本申请中的部分用语进行解释说明,以便于本领域技术人员理解。

[0059] (1) 超文本传输协议(HyperText Transfer Protocol,HTTP),它是一种用于分布式、协作式和超媒体信息系统的应⽤层协议,是万维网的数据通信的基础,也是互联网应⽤最为广泛的一种网络传输协议。最初设计HTTP的目的是为了提供一种发布和接收HTML页面的方法。

[0060] (2) 木马的命令与控制服务器(Command and Control Server,CC/C2):远程命令和控制服务器,目标机器可以接收来自服务器的命令,从而达到服务器控制目标机器的目的。该方法常用于病毒木马控制被感染的机器。

[0061] (3) 因特网中继聊天(Internet Relay Chat,IRC),一种应用层的协议,主要用于群体聊天。IRC用户使用特定的用户端聊天软件连接到IRC服务器,通过服务器中继与其他连接到这一服务器上的用户交流,所以IRC的中文名为“因特网中继聊天”。

[0062] (4) N-gram,n元语法,指文本中连续出现的n个语词。n元语法模型是基于(n-1)阶马尔可夫链的一种概率语言模型,通过n个语词出现的概率来推断语句的结构。

[0063] (5) Content-Type,内容类型,一般是指网页中存在的Content-Type,用于定义网络文件的类型和网页的编码,决定浏览器将以什么形式、什么编码读取这个文件,这就是经常看到一些网页点击的结果却是下载到的一个文件或一张图片的原因。ContentType属性指定响应的HTTP内容类型,如果未指定ContentType,默认为TEXT/HTML。

[0064] (6) 表示学习(Representation Learning),又称学习表示。在深度学习领域内,表示是指通过模型的参数,采用何种形式、何种方式来表示模型的输入观测样本X。表示学习指学习对观测样本X有效的表示。表示学习得到的低维向量表示是一种分布式表示(distributed representation)。之所以如此命名,是因为孤立地看向量中的每一维,都没有明确对应的含义;而综合各维形成一个向量,则能够表示对象的语义信息。

[0065] (7) 决策树(Decision Tree)是在已知各种情况发生概率的基础上,通过构成决策树来求取净现值的期望值大于等于零的概率,评价项目风险,判断其可行性的决策分析方法,是直观运用概率分析的一种图解法。由于这种决策分支画成图形很像一棵树的枝干,故称决策树。在机器学习中,决策树是一个预测模型,他代表的是对象属性与对象值之间的一种映射关系。分类树(决策树)是一种十分常用的分类方法。他是一种监督学习,所谓监督学习就是给定一堆样本,每个样本都有一组属性和一个类别,这些类别是事先确定的,那么通过学习得到一个分类器,这个分类器能够对新出现的对象给出正确的分类。这样的机器学习就被称之为监督学习。

[0066] (8) 用户代理(User Agent,UA),是指浏览器,还包括搜索引擎。它的信息包括硬件平台、系统软件、应用软件和用户个人偏好。

[0067] (9) 统一资源定位符(Uniform Resource Locator,URL),又叫做网页地址,是互联网上标准的资源的地址。互联网上的每个文件都有一个唯一的URL,它包含的信息指出文件

的位置以及浏览器应该怎么处理它。URL最初是由蒂姆·伯纳斯-李发明用来作为万维网的地址的。

[0068] (10) 内容类型,Content-Type,一般是指网页中存在的Content-Type,用于定义网络文件的类型和网页的编码,决定浏览器将以什么形式、什么编码读取这个文件,这就是经常看到一些Asp网页点击的结果却是下载到的一个文件或一张图片的原因。ContentType属性指定响应的HTTP内容类型,如果未指定ContentType,默认为TEXT/HTML。

[0069] (11) TF-IDF(Term Frequency-Inverse Document Frequency),是一种用于信息检索与数据挖掘的常用加权技术,用以评估一个字词对于一个文件集或一个语料库中的其中一份文件的重要程度。字词的重要性随着它在文件中出现的次数成正比增加,但同时会随着它在语料库中出现的频率成反比下降。TF-IDF加权的各种形式常被搜索引擎应用,作为文件与用户查询之间相关程度的度量或评级。除了TF-IDF以外,因特网上的搜索引擎还会使用基于链接分析的评级方法,以确定文件在搜寻结果中出现的顺序。

[0070] (12) 词袋模型(Bag-of-words,BOW),该Bag-of-words模型是信息检索领域常用的文档表示方法。在信息检索中,BOW模型假定对于一个文档,忽略它的单词顺序和语法、句法等要素,将其仅仅看作是若干个词汇的集合,文档中每个单词的出现都是独立的,不依赖于其它单词是否出现。(是不关顺序的)也就是说,文档中任意一个位置出现的任何单词,都不受该文档语意影响而独立选择的。

[0071] (13) ROC(Receiver Operating Characteristic Curve):接受者操作特征曲线。ROC曲线及AUC系数主要用来检验模型对客户进行正确排序的能力。ROC曲线描述了在一定累计好客户比例下的累计坏客户的比例,模型的识别能力越强,ROC曲线越往左上角靠近。AUC系数表示ROC曲线下方的面积。AUC系数越高,模型的风险区分能力越强。

[0072] (14) KS(Kolmogorov-Smirnov)检验:K-S检验主要是验证模型对违约对象的区分能力,通常是在模型预测全体样本的信用评分后,将全体样本按违约与非违约分为两部分,然后用KS统计量来检验这两组样本信用评分的分布是否有显著差异。

[0073] 基于上述提出的技术问题,也为了便于理解本申请实施例,下面先对本申请实施例所基于的其中一种恶意流量识别系统架构进行描述。请参阅图1,图1是本申请实施例提供的一种恶意流量识别系统构架示意图。本申请中的客户端可以包括图1中的第一服务设备001、第二服务设备002和第三服务设备003,其中,第一服务设备001、第二服务设备002和第三服务设备003之间可以通过有线或无线的方式进行通信连接,第二服务设备002和第三服务设备003均可以向第一服务设备发送超文本传输协议(HyperText Transfer Protocol,HTTP)请求。其中,

[0074] 第一服务设备001可以包括但不限于后台服务器、组件服务器、数据处理服务器等,为客户提供各种本地服务程序的设备。另外,第一服务设备001可以接收或响应一个或多个服务设备发送超文本传输协议(HyperText Transfer Protocol,HTTP)请求,以便为其他的服务设备提供相应的应用服务。但第一服务设备001需要识别出其他服务设备发送的HTTP请求是否属于恶意流量,若属于恶意流量,为了保证网络安全则不能对其响应。因此,第一服务设备001配置有恶意流量识别的本地服务,其中,该本地服务可包括但不限于:确定第一告警流量的接收时间;按照预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告

警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;对所述多条第二告警流量进行特征提取,获得第一特征信息;基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

[0075] 第二服务设备002也可以包括但不限于后台服务器、组件服务器、数据处理服务器等,为客户提供各种本地服务程序的设备。可以安装并运行相关的应用,可以向第一服务设备发送HTTP请求,以便第一服务设备响应后得到相应的服务。

[0076] 第三服务设备003,可以为木马的命令与控制服务器(Command and Control Server,CC/C2),其他服务设备可以接收来第三服务设备003(CC服务器)的命令,从而达到第三服务设备003控制上述服务设备的目的,常用于病毒木马控制被感染的服务设备。例如:在本申请实施例中,第三服务设备003可以向第一服务设备发送HTTP请求,使得第一服务设备接收到HTTP流,该HTTP流为恶意流量,可以被第一服务设备识别出。

[0077] 可以理解的是,图1中的网络架构只是本申请实施例中的一种示例性的实施方式,本申请实施例中的恶意流量识别系统架构包括但不限于以上恶意流量识别系统架构。

[0078] 基于图1提供的恶意流量识别系统架构,结合本申请中提供的恶意流量识别方法,对本申请中提出的技术问题进行分析解决。

[0079] 参见图2,图2是本申请实施例提供的一种恶意流量识别方法的流程示意图,该方法可应用于上述图1中所述的恶意流量识别系统架构中,其中的第一服务设备001可以用于支持并执行图2中所示的方法流程步骤S201-步骤S209。下面将结合附图2从第一服务设备侧进行描述。该方法可以包括以下步骤S201-步骤S209。

[0080] 步骤S201:接收多条第四HTTP流。

[0081] 具体的,恶意流量识别装置接收多条第四超文本传输协议HTTP流。其中,该第四HTTP流可以是第一服务设备接收到的来自一台或多台第二服务设备和/或第三服务设备发送的超文本传输协议HTTP流。

[0082] 步骤S202:对多条第四HTTP流中每一条第四HTTP流进行特征提取,获得第二特征集合。

[0083] 具体的,恶意流量识别装置对所述多条第四HTTP流中每一条第四HTTP流进行特征提取,获得第二特征集合,其中,所述第二特征集合包括:所述多条第四HTTP流分别对应的第二特征信息。可以理解的是,对于每一条第四HTTP流,第一服务设备001可以按照预设特征提取规则进行特征提取,然后会获的对应的非数字特征向量和其他的数字特征向量,将这些非数字特征向量和其他的数字特征向量按照统一的规则拼接起来,就得到了最终的单流特征向量,即,第四HTTP流对应的第二特征信息。请参考附图3,图3是本申请实施例提供的一种恶意流量识别的框架示意图。如图3所示,本申请实施例先对现网流量通过单流分类器(通过多条黑流量和白流量训练好的模型进行特征处理和单流分类(单流过滤)),获得疑似恶意流量的第一告警流量,例如:在单流的数据流量的基础上,通过特征处理器进行特征提取,提取流量中的单流特征形成特征向量,将此类特征向量输入分类器中,进行初步判断该流量是否是恶意软件的CC通信流量(即,第一告警流量);在基于该第一告警流量进行多流特征提取,获得多流特征表示(多流回溯);最后基于该多流特征表示通过回溯模型和基线模型确定该第一告警流量是否为恶意流量。另外,还可以进一步的使用上述模型提取的特征通过恶意家族分类器,最终确定第一告警流量所属类型。其中,具体的实现方式可参考

下述步骤,本申请实施例在此暂不描述。

[0084] 可选的,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。

[0085] 例如:请参考附图4,图4是本申请实施例提供的一种特征提取的示意图。如图4所示,可以对于接收到的多条第四HTTP流,分别采用特征工程方法提取手工特征和表示学习方式特征提取。其中,(1)手工特征信息包括以下特征中的一个或多个:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征(HTTP响应特征);其中,URL统计特征包括以下特征中的一个或多个:长度,元音比例,辅音比例,特殊字符比例,大写字母比例,小写字母比例,数字比例,域名级数,域名字符分布,顶级域名,路径(path)长度,path层数,文件后缀,参数个数,平均参数值长度,是否存在base64,是否遵从常见模式;HTTP Header特征包括以下特征中的一个或多个:内容类型Content Type,用户代理UA,HTTP返回状态码,Header序列的N-gram。(2)表示学习特征信息为以表示学习(Representation Learning)的方式作为辅助,在神经网络输出层之前,抽取第四HTTP流的高维特征,最大化地对已有数据集进行特征抽取,并在较高维度上进行关联。其中,图4所示的白流量指代正常流量,黑流量指代恶意流量。将多条第四HTTP流中每一条第四HTTP流进行特征提取(手工特征提取和表示学习特征提取),对提取的特征进行预处理(如:数字特征处理和非数字特征转换),再将特征组合和筛选后,获得第二特征集合。

[0086] 可选的,所述对多条第四HTTP流中每一条第四HTTP流进行特征提取,获得第二特征集合,包括:对多条第四HTTP流中每一条第四HTTP流进行特征提取,获得初始特征集合;对所述初始特征集合内非数字特征进行文本处理,获得所述第二特征集合。需要说明的是,由于分类模型一般处理数字输入,所以对于特征中的文本特征或非数字特征需要进行文本-数字转换,将其转换为分类模型可以处理的数字化向量。其中,对多条第四HTTP流中每一条第四HTTP流进行特征提取的方式可以通过手工特征提取和/或表示学习特征提取的方式。

[0087] 可选的,上述涉及的文本特征包括但不限于:顶级域名,文件后缀,Content Type,UA等。可以理解的是,由于这四个字段特征的输入均是字符串,而机器学习分类器无法处理字符串,所以需要字符串进行转换,将其转换为分类模型可以处理的数字化向量。上述文本处理过程使用的方法为:TF-IDF。其中,TF-IDF中的“词频”(Term Frequency,缩写为TF),TF=某个词在文章中出现的次数,体现的是一个词在文档中出现的频率,“逆文档频率”(Inverse Document Frequency,缩写为IDF),IDF=某个词在文章中的出现次数/文章的总词数,体现的是一个词常见程度的反比,可以有效的解决一些出现频率比较高但是并没有很大的意义的词。在本申请实施例中,可以使用 $TF-IDF = TF * IDF$ 的方法,有效地体现在流量中一个字段中某一个字符串出现的频率。例如:首先对这些特征进行TF-IDF转换,基于词频和文档顺序计算出其向量表达。需要说明的是,在分类识别的过程中,利用TF-IDF处理的数据需要与检测模型的基础TF-IDF库进行对比发现异常,基础TF-IDF库可以在训练过程中由白流量(可以指利用某些技术手段可以确认识别的正常数据流量,用于模型训练或者正确性验证)统计获得,可以在一个具体检测场景下利用具体白流量生成。

[0088] 在一种可能实现的方式中,对所述初始特征集合内非数字特征进行文本处理,获得所述第二特征集合,包括:对所述初始特征集合内非数字特征进行文本处理,获得数字特征向量集合;对上述数字特征向量集合进行降维处理,获得所述第二特征集合。可以理解的是,对提取到的初始特征集合进行TF-IDF处理后,得到的向量维度比较大,这样高维的向量对于分类模型和后续的处理都比较消耗资源,并且处理效率不高,因此,可以进行降维处理将这样的—个高维向量转换到低维向量空间。其中,该降维处理的方法可以包括但不限于奇异值分解(Singular value decomposition,SVD)、主成分分析(Principal Component Analysis,PCA)等。例如,在本申请实施例中,由于TF-IDF计算后的向量维度过大,容易出现维度爆炸的问题,所以进行降维操作,将TF-IDF处理后的向量从高维空间降低到一个十维的空间中。

[0089] 可选的,对每条第四HTTP流使用不同方法提取的特征进行组合和筛选,获得每条第四HTTP流对应的第二特征信息。例如:将特征工程特征和表示学习特征进行组合,并通过最小冗余最大相关性(mRMR)等特征选择算法,筛选出每条第四HTTP流对应的效果最优的特征集。如上述图4所示,本申请实施例,在从现网流量中提取单流的流量特征,对非数字特征进行文本处理,对流量特征进行组合和筛选从而获得第二特征集合。

[0090] 步骤S203:基于第二特征集合,通过第一分类模型,从多条第四HTTP流中筛选出第一告警流量。

[0091] 具体的,恶意流量识别装置可以基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。其中,第一告警流量为通过第一分类模型从所述多条第四HTTP流中筛选出疑似恶意流量的流量。例如:将上述得到的每一条第四HTTP流的流量特征向量(即,第二特征信息),输入进第一分类模型中。第一分类模型可采用stack模式,基于不同的特征训练不同的分类器进行判定,第一分类模型可以用于基于每个分类器的判定结果利用决策树机制最终可以得到基于HTTP会话的第一层检测结果。另外,该第一分类模型可以是利用已经标记好的黑白流量训练数据集训练得到的模型。这种对数据进行预处理实现对正常流量的初始筛选。在此基础上,面向单流的数据流量基于人工经验和表示学习的方法进行复合特征的抽取与选择,形成单流特征向量,然后将此类特征向量输入分类器中,进行第一步判断该流量是否疑似恶意软件的CC通信流量,若是,再进一步的进行下一步的判断,大大提升了判断该流量是否是恶意流量的效率。

[0092] 步骤S204:确定第一告警流量的接收时间。

[0093] 具体的,恶意流量识别装置确定第一告警流量的接收时间。在筛选出第一告警流量后可以确定第一告警流量的接收时间,以便回溯多条流量。

[0094] 步骤S205:按照预设策略获取目标时间段内与第一告警流量对应的多条第二告警流量。

[0095] 具体的,恶意流量识别装置按照预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量,所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值。在检测过程中,由于现网中流量情况相对较为复杂,针对单条HTTP流的检测具备一定的偶然性,如果能从多流角度对恶意样本通信行为进行观察,将多个请求基于不同的方法回溯到不同簇,利用每条告警流所属不同簇的统计特征组合,研判正负性,从而杜绝了偶然误差。即,观

察恶意样本在一定时间内整体的通信行为,就可以从行为角度更准确的判断恶意样本,使得最终的多流结果更为鲁棒,同时具备行为上的可解释性。

[0096] 可选的,所述目标时间段为基于所述接收时间确定的时间段,例如:所述目标时间段为以所述接收时间为起点向后预设时长的时间段,或者为以所述接收时间为终点向前预设时长的时间段。又例如:目标时间段还可以为包括接收时间的时间段。在接收第一告警流量附近获取第二告警流量,可以保证获得尽可能多的与第一告警流量相似的多条第二告警流量。

[0097] 可选的,所述预设策略包括:第一策略、第二策略、第三策略中的一个或多个,其中,所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略;所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略;所述第三策略为基于所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。其中,在原有检测方法的基础上,在第一分类模型报出结果后,使用流量回溯方法,基于第一告警流量向前和/或向后采集一段时间的CC通信流量,然后进行多流特征提取。可以理解的是,第一策略是基于第一告警流量的IP地址和UA信息进行回溯,可以回溯到同个软件、同个服务设备或同个应用发送的多条流量;第二策略是基于第一告警流量的IP地址回溯多条流量,然后按照预设的泛化规则泛化回溯到的流量,从而筛选出与第一告警流量同个软件不同应用发送的多条流量;第三策略是基于第一告警流量的IP地址和HTTP Header信息进行回溯,可以回溯到同个软件中不同应用发送的多条流量。多种流量回溯方式均可以精准的回溯到第一告警流量同源的多条流量,从而可以根据该多条流量的行为特征识别出第一告警流量是否为恶意流量,提高了识别恶意流量的精准度。

[0098] 可选的,所述预设策略包括所述第一策略;所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的IP地址和UA信息;采集在所述目标时间段内所述IP地址发送的多条HTTP流中,与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。请参考附图5,图5是本申请实施例提供的一种按照第一策略回溯流量的流程示意图。如图5所示,若预设策略包括第一策略,即可以使用第一告警流量的UA信息和源IP地址信息作为唯一索引进行流量回溯,通过UA Header信息进行应用流量标识,抽取出所述源IP地址(src-ip)前N分钟或后N分钟发出的相同UA信息的所有HTTP流为第二告警流量进行回溯分析。通过该方式可以回溯到同个软件、同个服务设备或同个应用发送的多条流量,提高了识别恶意流量的准确率。请参考附图6,图6是本申请实施例提供的一种根据第一策略回溯的多条流量示意图。如图6所示,根据3条第一告警流量,按照第一策略,回溯了十条HTTP请求,其中,该10条HTTP请求根据IP地址信息和UA信息共分为三组分别对应3条第一告警流量。多流分组1对应IP地址为IP、UA信息为UA1的第一告警流量;多流分组2对应IP地址为IP、UA信息为UA2的第一告警流量;多流分组3对应IP地址为IP、UA信息为UA3的第一告警流量。另外,HTTP请求1-HTTP请求4:对应了典型站点轮询+URL变化模式;HTTP请求5-HTTP请求7:对应了典型稳定心跳模式;HTTP请求8-HTTP请求10:对应了特定的一些样本通信行为。

[0099] 可选的,所述预设策略包括所述第二策略,所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的所述IP地

址;采集在所述目标时间段内所述IP地址发送的多条第一HTTP流;对多条第一HTTP流按照所述预设泛化规则进行泛化处理,获得多条第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于所述预设阈值的第二HTTP流为所述第二告警流量。请参考附图7,图7是本申请实施例提供的一种按照第二策略回溯流量的流程示意图。如图7所示,通过对形成的流量进行泛化,将其产生变化的字段用字符代替,对相同源IP发出的流量进行统一泛化,并计算模板之间的字符串相似度,从而在源IP的历史流量(如:相同源IP在目标时间段内的流量数据)中匹配出最相似的所有HTTP流,即为第二告警流量。其中,所谓泛化,是对流量中的变化字符串位置,使用同一标准进行替换(如本申请实施例中,可以将所有小写字母换为x,特殊字符换为T,大写字母换为X)。请参考附图8,图8是本申请实施例提供的一种流量泛化前后的示意图。如图8所示,多条第一HTTP流按照统一的泛化规则进行泛化后,获得了其分别对应的第二HTTP流。进一步的,可以计算多条第二HTTP流与第一告警流量之间的相似度。这种通过泛化后,计算流量之间相似度的方法,进而确定与第一告警流量同簇的(同个软件、不同应用发送的)多条流量(相似度超过预设阈值),进而根据该多条流量的行为特征确定第一告警流量是否为恶意流量,提高了识别恶意流量的准确度。

[0100] 可选的,从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于所述预设阈值的第二HTTP流为所述第二告警流量,包括:将所述多条第二HTTP流向量化,再计算向量化后的多条第二HTTP流与第一告警流量之间的相似度。其中,恶意流量识别装置可以首先使用词袋模型(BOW)来向量化,再使用向量空间模型(VSM)中的余弦相似度分别计算多条第二HTTP流与第一告警流量之间的相似度。进行字符串相似性度量的时候,求得两个泛化后请求在同一BOW下的向量表示,并计算余弦距离(相似度)。其中,流量间的相似度计算可以使用向量空间模型(VSM)中的余弦相似度:向量空间模型是一个把文本文件表示为标识符(比如索引)向量的代数模型。它应用于信息过滤、信息检索、索引以及相关排

序。
$$\text{similarity} = \cos(\theta) = \frac{A \cdot B}{\|A\| \|B\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}}$$
其中,A为告警流的模板向量,B为回溯流的向量。

[0101] 可选的,所述预设策略包括所述第三策略,所述按照预设策略采集目标时间段内与所述第一告警流量对应的多条第二告警流量,包括:获取所述第一告警流量的所述IP地址和所述HTTP Header信息;采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;基于所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。请参考附图9,图9是本申请实施例提供的一种按照第三策略回溯流量的流程示意图。如图9所示,对源IP的HTTP请求的HTTP Header进行N-gram处理,即,提取流量中的HTTP Header序列(sequence)信息,分别对N取不同值(视性能考虑),形成以下表1所示样本-头部组合矩阵(HTTP header sequence N-gram矩阵)。使用Hash Trick进行降维,提取降维后同序列的HTTP流。

[0102] 表1, HTTP header sequence N-gram矩阵

样本	header n-gram seq 1	header n-gram seq 2	header n-gram seq 3	header n-gram seq 4	header n-gram seq 5	header n-gram seq 6	header n-gram seq 7
sample 1	1	0	0	0	0	0	1
sample 2	0	1	0	0	0	0	0
sample 3	1	0	0	0	1	0	1
sample 4	1	0	0	0	1	0	0
... ..							

[0104] 其中,如图9所示,由于组合矩阵维度较高,可以采用hash trick方式对矩阵进行降维,获得N-gram矩阵降维后的矩阵。例如:对特征向量x进行随机转换进行一次MinHash,得到哈希结果,取哈希结果(可以用二进制表示)的最后b位。就是b-bit Min Hash的过程。该过程重复k次,每个样本就可以用k*b位进行表示,处理的时间和空间要求大大降低。这种通过提取流量(如:相同源IP在目标时间段内的流量数据)中的HTTP Header序列信息进行回溯的方法,可以回溯到同个软件中不同应用发送的多条流量,进而根据该多条流量的行为特征确定第一告警流量是否为恶意流量,提高了识别恶意流量的准确度。

[0105] 步骤S206:对多条第二告警流量进行特征提取,获得第一特征信息。

[0106] 具体的,所述恶意流量识别装置对多条第二告警流量进行特征提取,获得第一特征信息。可以理解的是,按照上述一种或多种策略回溯方法得到的HTTP流,分别输入下一阶段进行特征的提取。分别获取一种或多三种回溯方法得到的多条HTTP流对应的表示向量,并将其连接为一个向量,即为第一特征信息。请参考附图10,图10是本申请实施例提供的一种获得第一特征信息的方法流程示意图。如图10所示,通过单流分类器获得第一告警流量,即预分类结果;根据该第一告警流量通过第一策略(即,UA聚合)、第二策略(即,流量模板相似聚类)和/或第三策略(HTTP header N-gram)后回溯的多条第二告警流量(多流数据),对该多条第二告警流量进行特征提取,获得每种策略对应的特征表示向量(Vector-traceback),再将其组合成的多流特征表示向量即为第一特征信息。

[0107] 可选的,所述第一特征信息为特征表示向量;所述对所述多条第二告警流量进行特征提取,获得第一特征信息,包括:对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;根据所述行为特征信息,获取所述特征表示向量。可以使得恶意流量识别装置对流量进行识别时,充分考虑恶意CC通信流量的多流网络行为的特征,可以更加精准的检测并分辨现网中的恶意流量。需要说明的是,请参考下述表格2,表2是本申请实施例提供的一种多流的行为特征信息表。

[0108] 表2,多流模型特征说明

特征分类	特征名称	特征描述
[0109]	连接行为特征	回溯时间段内的连接次数
		连接时间间隔序列
		连接时间间隔 max
		连接时间间隔 min
		连接时间间隔均值
		连接时间间隔方差
		连接包大小序列
		连接包大小 max
[0110]		连接包大小 min
		连接包大小均值
		连接包大小方差
	请求差异特征	请求参数差异
		请求参数熵值
		请求资源类型/请求文件类型
	请求响应特征统计	返回包相同大小包的占比
		返回包大小序列
		返回包大小 max
		返回包大小 min
		返回包大小均值

[0111] 步骤S207:基于第一特征信息,判断第一告警流量是否为恶意流量。

[0112] 具体的,恶意流量识别装置可以基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。第一特征信息可以用于表征第一告警流量对应多流流量的行为特征信息,基于该行为特征信息,通过回溯模型进行检测,可以判断第一告警流量是否为恶意流量。例如,将得到的多流的行为特征信息,如:向量表示形式,输入进上述回溯模型(多流分类器),另外,为了高度利用向量特征,可以采取stacking的方式进行多次训练提取向量的行为特征,即可以得到基于该回溯模型多得到检测结果。其中,所述回溯模型可以为预先训练好的,用于识别流量是否为恶意流量的分类模型。

[0113] 可选的,所述根据所述第一特征信息,判断所述第一告警流量是否为恶意流量,包括:基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。其中,针对现网生产环境进行一段时间的流量数据积累,并在此基础上抽取现网流量的多流特征,以此为训练数据,构建现网历史数据的单分类模型(即,所述基线模型),使得此模型可以表示现网的行为基线,从而能够从基线的角度,对不同于常规行为的流量进行判别。另外,所述回溯模型可以为预先训练好的多流分类器,用于识别流量是否为恶意流量。然后,将回溯模型的第一检测结果 $y_1(x)$ 与通过历史流量预训练的单分类基线异常检测模型的第二检测结果 $y_2(x)$ 进行平滑性整合,得到最终的判别结果 $Y(x)$ 。通过裁决公式得到其最终整合值,最后根据判别结果 $Y(x)$,确定第一告警流量是否为恶意流量。

具体的所述裁决公式为: $Y(x) = \text{sigmoid}(\frac{a_1 y_1(x) + a_2 y_2(x)}{2})$,其中,

$a_n = \ln(\frac{1-E_n}{E_n})$, $E_n = \frac{\text{amount(wrong predicts)}}{\text{amount(all samples)}}$,请参考附图11,图11是本申请实施例提供的一种

以 E_n 为自变量, a_n 为因变量的函数图像,其中 $E_n \in (0, 1)$ 。如图11所示,当错误率 E_n 越大时, a_n 向减小方向延伸,从而导致相应模型的判断权重减小。权重值与不同模型的输出值在经过算数平均后,输入平滑符号函数sigmoid进行最终映射值的计算,从而得到0(白样本标签或正常流量标签)和1(黑样本标签或恶意流量标签)的输出结果。另外,通过综合考虑通过回溯模型进行检测的第一检测结果和通过基线模型进行检测的第二检测结果,最终确定第一告警流量是否为恶意流量,大大提高了恶意流量识别的准确度。

[0114] 步骤S208:若第一告警流量为恶意流量,对第一告警流量进行预设泛化处理,获得泛化后的第一告警流量。

[0115] 具体的,若第一告警流量为恶意流量,恶意流量识别装置对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量。可以理解的是,若确实确定第一告警流量为恶意流量后,还可以识别该恶意流量属于哪一类的恶意流量。

[0116] 步骤S209:将泛化后的第一告警流量进行分类,确定第一告警流量匹配的恶意流量类型。

[0117] 具体的,恶意流量识别装置将泛化后的第一告警流量进行分类,确定第一告警流量匹配的恶意流量类型。其中,恶意流量识别装置通过训练好的种类分类模型对泛化后的第一告警流量进行分类,该识别恶意流量所属种类所用的分类模型为对已知恶意样本进行通信流量进行泛化处理后,使用上述步骤S207中涉及的模型(回溯模型)提取的特征训练完成的多家族分类模型,用于对恶意流量研判所属家族。因此,请参考附图12,图12是本申请实施例提供的一种确定恶意流量所属种类的流程示意图。如图12所示,恶意流量样本,通过泛化处理、提取流量模板、表示学习、特征提取、特征标识和多分类器后,可以确定告警流量匹配的恶意流量类型。即在本申请实施例中,恶意流量识别装置对所述第一告警流量进行预设泛化处理后,获得泛化后的第一告警流量,对该泛化后的第一告警流量进行特征提取(相当于特征抽取),获得对应的特征表示向量;最后将该特征表示向量输入上述的多家族分类模型,识别出恶意流量的类型。

[0118] 实施第一方面的实施例,恶意流量识别装置可以从单条流量(即:第一告警流量)的接收时间起,按照预设策略回溯目标时间段内与该单条流量匹配的多条流量(即:多条第二告警流量)。然后,对回溯到的多条流量进行特征提取,获得特征信息,使得恶意流量识别装置可以根据该特征信息对上述单条流量进行分类,从而确定该单条流量是否为恶意流量。其中,该多条第二告警流量与第一告警流量之间的相似度均大于预设阈值。这种根据单条流量相似的多条流量的特征信息对单条流量进行分类的方法,使得恶意流量识别装置对流量进行识别时,可以充分考虑恶意CC通信流量的多流网络行为的特征,从而更加精准的检测并分辨现网中的恶意流量。避免了现有技术检测过程中,由于现网中流量情况相对较为复杂,针对单条HTTP流的检测具备的偶然性。另外,本申请实施例从多流角度对流量的通信行为进行观察,将多个告警流量基于一种或多种的方法回溯到不同簇,利用每条告警流所属不同簇的统计其特征信息,根据该特征信息研判正负性(即,告警流量是否为恶意流量),从而杜绝了偶然误差。这种观察恶意流量在一定时间内整体的通信行为,可以从行为角度判断恶意样本,使得最终的多流判断结果更为鲁棒,同时也具备行为上的可解释性。而且,本申请实施例对于多流流量无论是从流量层对应的特征来检测,还是从主机行为对应的特征来检测,基础信息丰富度都足够恶意流量识别装置有效准确的识别流量是否为恶意流量。从而,可以从多流的特征上区分流氓软件的通信流量和恶意软件的通信流量,提高恶意流量识别的准确率。

[0119] 另外,在针对某X校园网采集到的1600万条正常现网数据和1万多的恶意流量样本数据,分别使用现有技术和本申请实施例进行网络数据识别的应用场景下,获得以下实验数据。

[0120] 1、仅使用现有技术中单流检测模型:

[0121] 请参考下述表3,表3本申请实施例提供的一种单流模型性能数据表,然而基于威胁情报等侧面确认,在实际的网络运行中检测算法精度估计可以在80%左右。(上述某X校园网确认40多条流告警)

[0122] 表3,单流模型性能数据表

[0123]	Accuracy准确性	0.9999664730928924
	F1	0.9999831782138391
	Precision精密度	0.9999728493273421
	Recall检索率	0.999993507313716

[0124] 其中,表3说明了针对所有HTTP通信,实验环境(测试集)下ACC值达到99.99%以上,ROC值接近于1(0.99999)。其中,ROC值一般在0.5-1.0之间。值越大表示模型判断准确性越高,即越接近1越好。ROC=0.5表示模型的预测能力与随机结果没有差别。KS值表示了模型将加和减区分开来的能力。KS值越大,模型的预测准确性越好。一般,KS>0.2即可认为模型有比较好的预测准确性。

[0125] 2、使用本申请实施例中所述恶意流量识别方法

[0126] 在单层检测模型基础上进行多流判定,实验环境下成功发现现网IP聚集感染行为,在所有最终告警样本中,某X校园网的回溯模型的识别精度达到100%。请参考下述表4中检测出的恶意流量样例,如下表4中检测到的IP地址为166.***.**.111和166.***.**.191的两簇恶意HTTP流。

[0127] 表4, 恶意流量样本数据

[0128]	http://arimaexim.com/logo.gif?f5da****=-119****187	158****498	166.***.**.111
	http://arimaexim.com/logo.gif?faa7****=-89****66	158****025	166.***.**.111
	http://arimaexim.com/logo.gif?f69c****=-110****150	158****218	166.***.**.111
	http://www.arimaexim.com/logo.gif?faa7****=-89****66	158****026	166.***.**.111

	http://ampyazilim.com.tr/images/xs2.jpg?cdd****=21****164	158****717	166.***.**.191
	http://ahmediye.net/xs.jpg?857****=559****96	158****826	166.***.**.191

[0129] 综上所述, 实施本申请实施例, 可以首先基于多流回溯的流量分离方法, 准确分离连续时间段下的同一恶意软件/应用通信的HTTP流量; 其次, 基于回溯的多级检测框架(先单流过滤再多流回溯)可以有效降低检测过程中对大量无关数据流的存储与检测(回溯流量只需要第一层检测出的可疑流量, 占比很小), 提高分析效率, 更适合应用在企业网环境。另外, 基于多流回溯的流量分离方法, 从多流行为特征上区分流氓软件的通信流量和恶意软件的通信流量。

[0130] 上述详细阐述了本申请实施例的方法, 下面提供了本申请实施例的相关装置。

[0131] 请参见图13, 图13是本申请实施例提供的一种恶意流量识别装置的结构示意图, 该恶意流量识别装置10可以包括确定单元101、回溯单元102、提取单元103和判断单元104, 还可以包括: 泛化单元105、分类单元106和告警流量单元107。其中, 各个单元的详细描述如下。

[0132] 确定单元101, 用于确定第一告警流量的接收时间;

[0133] 回溯单元102, 用于按照预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量; 所述目标时间段为基于所述接收时间确定的时间段; 所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;

[0134] 提取单元103, 用于对所述多条第二告警流量进行特征提取, 获得第一特征信息;

[0135] 判断单元104, 用于基于所述第一特征信息, 判断所述第一告警流量是否为恶意流量。

[0136] 在一种可能实现的方式中, 所述预设策略包括: 第一策略、第二策略、第三策略中的一个或多个, 其中, 所述第一策略为基于所述第一告警流量的网际协议IP地址和用户代理UA信息获取所述多条第二告警流量的策略; 所述第二策略为基于所述第一告警流量的IP地址和预设泛化规则获取所述多条第二告警流量的策略; 所述第三策略为基于所述第一告警流量的IP地址和所述第一告警流量的超文本传输协议HTTP Header信息获取所述多条第二告警流量的策略。

[0137] 在一种可能实现的方式中, 所述预设策略包括所述第一策略; 所述回溯单元102, 具体用于: 获取所述第一告警流量的IP地址和UA信息; 采集在所述目标时间段内所述IP地址发送的多条HTTP流中, 与所述第一告警流量的UA信息相同的HTTP流为所述第二告警流量。

[0138] 在一种可能实现的方式中, 所述预设策略包括所述第二策略, 所述回溯单元102, 具体用于: 获取所述第一告警流量的所述IP地址; 采集在所述目标时间段内所述IP地址发送的多条第一HTTP流; 对多条第一HTTP流按照所述预设泛化规则进行泛化处理, 获得多条

第二HTTP流,所述预设泛化规则为对所述多条第一HTTP流中每一条第一HTTP流对应的目标字符串,使用预设标准进行统一替换;从所述多条第二HTTP流中,筛选出与所述第一告警流量之间相似度大于预设阈值的目标第二HTTP流为所述第二告警流量。

[0139] 在一种可能实现的方式中,所述预设策略包括所述第三策略,所述回溯单元102,具体用于:获取所述第一告警流量的所述IP地址和所述HTTP Header信息;采集在所述目标时间段内所述IP地址发送的多条第三HTTP流;分别对所述多条第三HTTP流中每一条第三HTTP流对应的HTTP Header进行N-gram处理,获得第一矩阵,所述第一矩阵包括所述每一条第三HTTP流对应的HTTP Header序列信息;对所述第一矩阵进行降维处理,提取降维处理后的第一矩阵中与所述第一告警流量的HTTP Header信息匹配的目标HTTP Header序列信息;基于所述目标HTTP Header序列信息,获取所述目标HTTP Header序列信息对应的第三HTTP流为所述第二告警流量。

[0140] 在一种可能实现的方式中,所述第一特征信息为特征表示向量;所述提取单元103,具体用于:对所述多条第二告警流量进行特征提取,获得所述多条第二告警流量对应的行为特征信息,所述行为特征信息包括:连接行为特征,请求差异特征,请求响应特征中的一个或多个;根据所述行为特征信息,获取所述特征表示向量。

[0141] 在一种可能实现的方式中,所述判断单元104,具体用于:基于所述第一特征信息通过回溯模型进行检测,获得第一检测结果;基于所述多条第二告警流量通过基线模型进行检测,获得第二检测结果,其中,所述基线模型是基于历史流量预先训练好的检测模型;基于所述第一检测结果和所述第二检测结果,判断所述第一告警流量是否为恶意流量。

[0142] 在一种可能实现的方式中,所述装置还包括:泛化单元105,用于若所述第一告警流量为恶意流量,对所述第一告警流量进行预设泛化处理,获得泛化后的第一告警流量;分类单元106,用于将所述泛化后的第一告警流量进行分类,确定所述第一告警流量匹配的恶意流量类型。

[0143] 在一种可能实现的方式中,所述装置还包括告警流量单元107,所述告警流量单元107,用于:确定第一告警流量的接收时间之前,接收多条第四HTTP流;对所述多条第四HTTP流中每一条第四HTTP流按照预设特征提取规则进行特征提取,获得第二特征集合,所述第二特征集合包括:所述多条第四HTTP流分别对应的第二特征信息;基于所述第二特征集合,通过第一分类模型,从所述多条第四HTTP流中筛选出所述第一告警流量。

[0144] 在一种可能实现的方式中,所述第二特征信息包括手工特征信息和/或表示学习特征信息;其中,所述手工特征信息包括:第四HTTP流对应的域名可读性特征、统一资源定位符URL结构特征、行为指示特征、HTTP Header特征中的一个或多个;所述表示学习特征信息包括第四HTTP流对应的高维特征。

[0145] 需要说明的是,本申请实施例中所描述的恶意流量识别装置10中各功能单元的功能可参见上述图2中所述的方法实施例中步骤S201-步骤S209的相关描述,此处不再赘述。

[0146] 如图14所示,图14是本申请实施例提供的另一种恶意流量识别装置的结构示意图,该装置20包括至少一个处理器201,至少一个存储器202、至少一个通信接口203。此外,该设备还可以包括天线等通用部件,在此不再详述。

[0147] 处理器201可以是通用中央处理器(CPU),微处理器,特定应用集成电路(application-specific integrated circuit,ASIC),或一个或多个用于控制以上方案程

序执行的集成电路。

[0148] 通信接口203,用于与其他设备或通信网络通信,如以太网,无线接入网(RAN),核心网,无线局域网(Wireless Local Area Networks,WLAN)等。

[0149] 存储器202可以是只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、只读光盘(Compact Disc Read-Only Memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0150] 其中,所述存储器202用于存储执行以上方案的应用程序代码,并由处理器201来控制执行。所述处理器201用于执行所述存储器202中存储的应用程序代码。

[0151] 存储器202存储的代码可执行以上图2提供的网络流量识别方法,比如确定第一告警流量的接收时间;按照预设策略获取目标时间段内与所述第一告警流量对应的多条第二告警流量;所述目标时间段为基于所述接收时间确定的时间段;所述多条第二告警流量中每条第二告警流量与所述第一告警流量的相似度均大于预设阈值;对所述多条第二告警流量进行特征提取,获得第一特征信息;基于所述第一特征信息,判断所述第一告警流量是否为恶意流量。

[0152] 需要说明的是,本申请实施例中所描述的恶意流量识别装置20中各功能单元的功能可参见上述图2中所述的方法实施例中的步骤S201-步骤S209相关描述,此处不再赘述。

[0153] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中未详述的部分,可以参见其他实施例的相关描述。

[0154] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本申请并不受所描述的动作顺序的限制,因为依据本申请,某些步骤可能可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本申请所必须的。

[0155] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如上述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

[0156] 上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0157] 另外,在本申请各实施例中的各功能单元可以集成在一个处理单元中,也可以是

各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0158] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以为个人计算机、服务端或者网络设备等,具体可以是计算机设备中的处理器)执行本申请各个实施例上述方法的全部或部分步骤。其中,而前述的存储介质可包括:U盘、移动硬盘、磁碟、光盘、只读存储器(Read-Only Memory,缩写:ROM)或者随机存取存储器(Random Access Memory,缩写:RAM)等各种可以存储程序代码的介质。

[0159] 以上所述,以上实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,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申请各实施例技术方案的精神和范围。

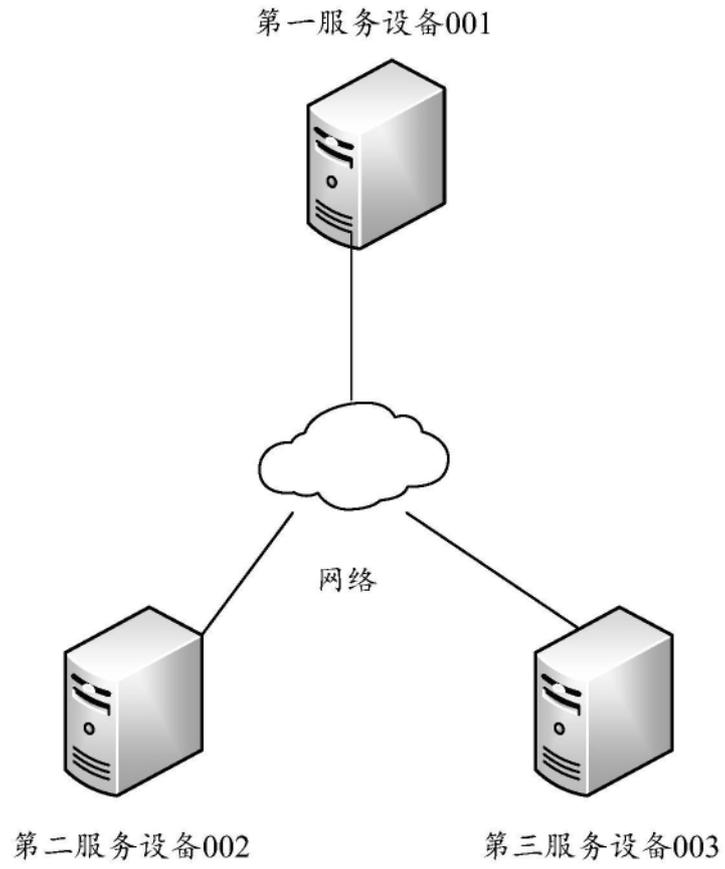


图1

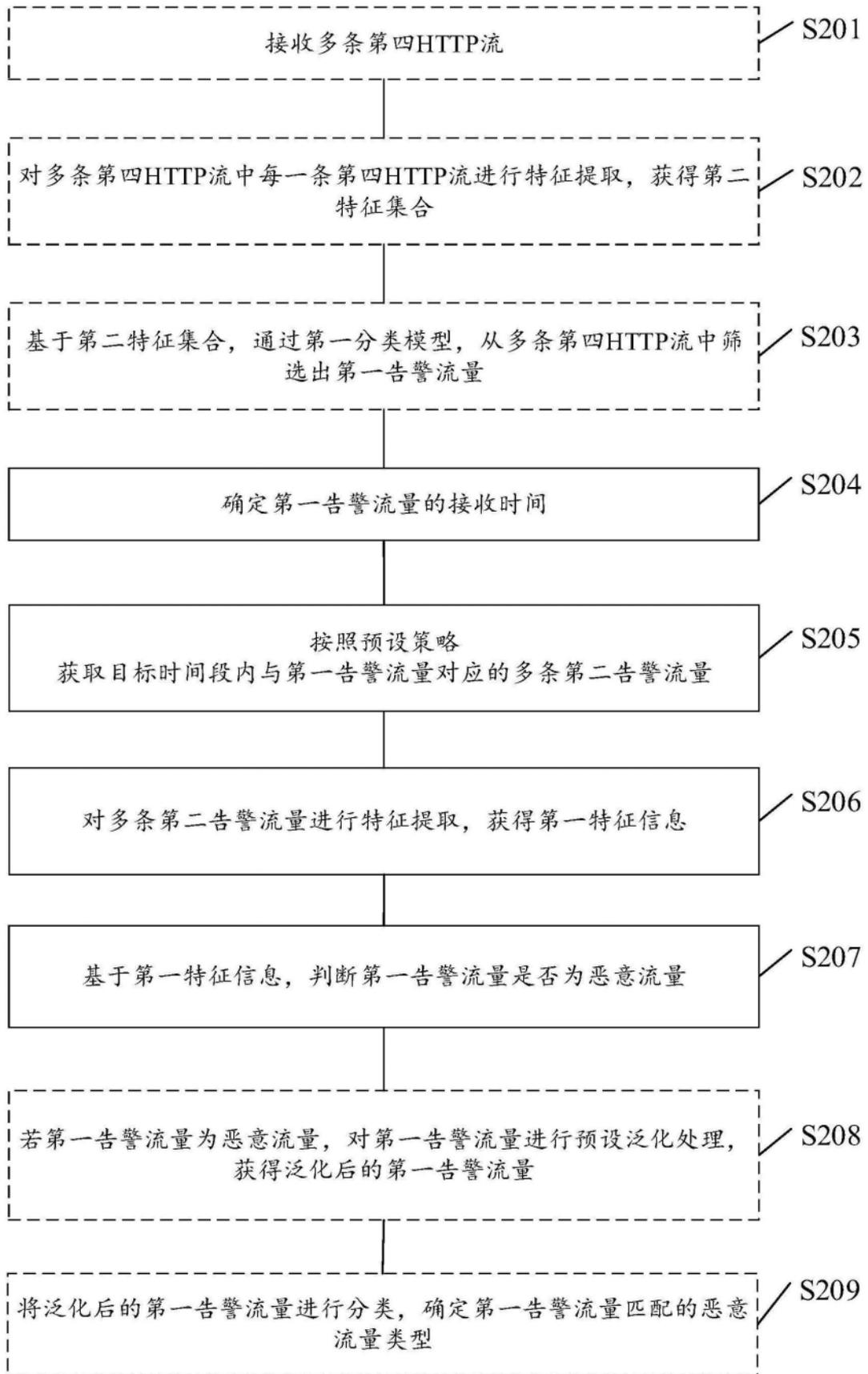


图2

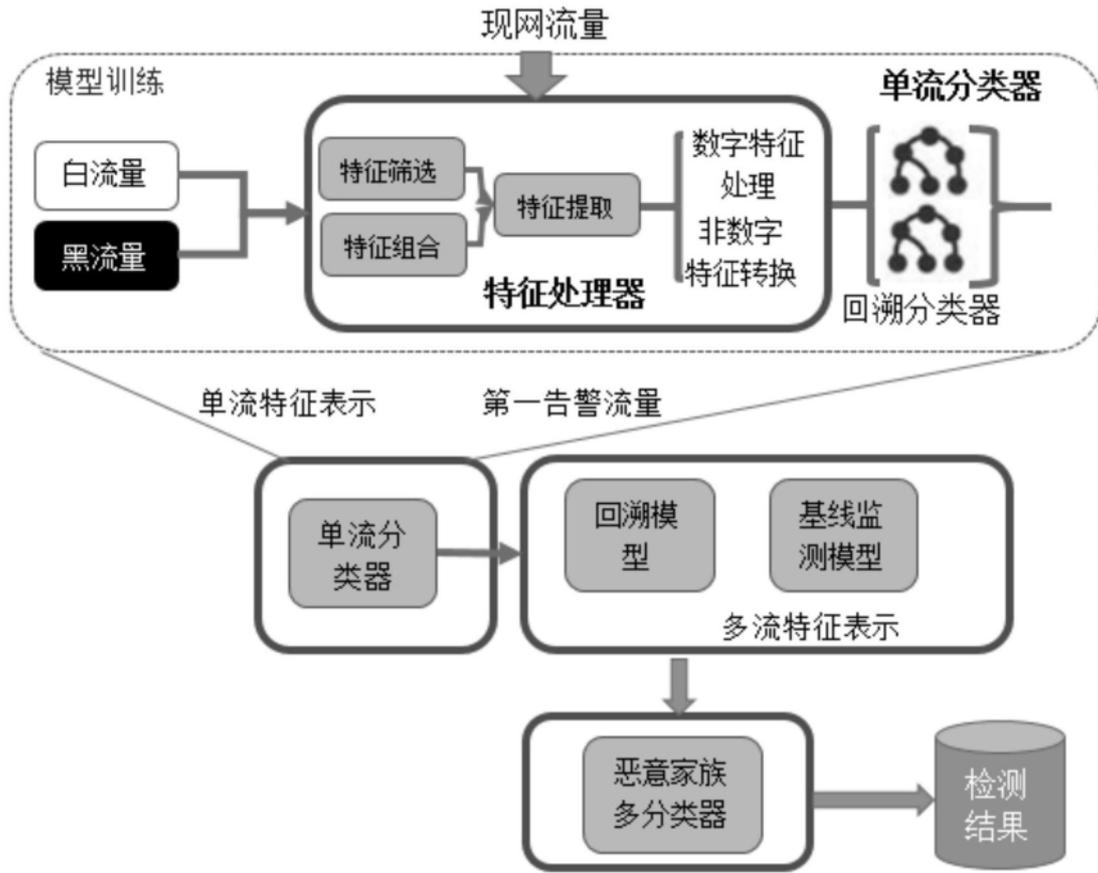


图3

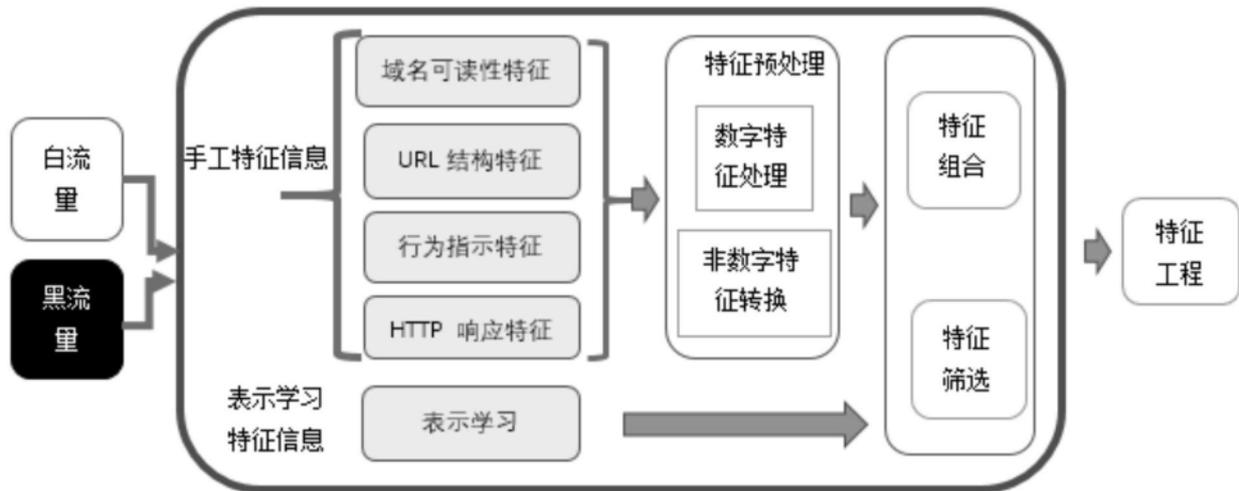


图4

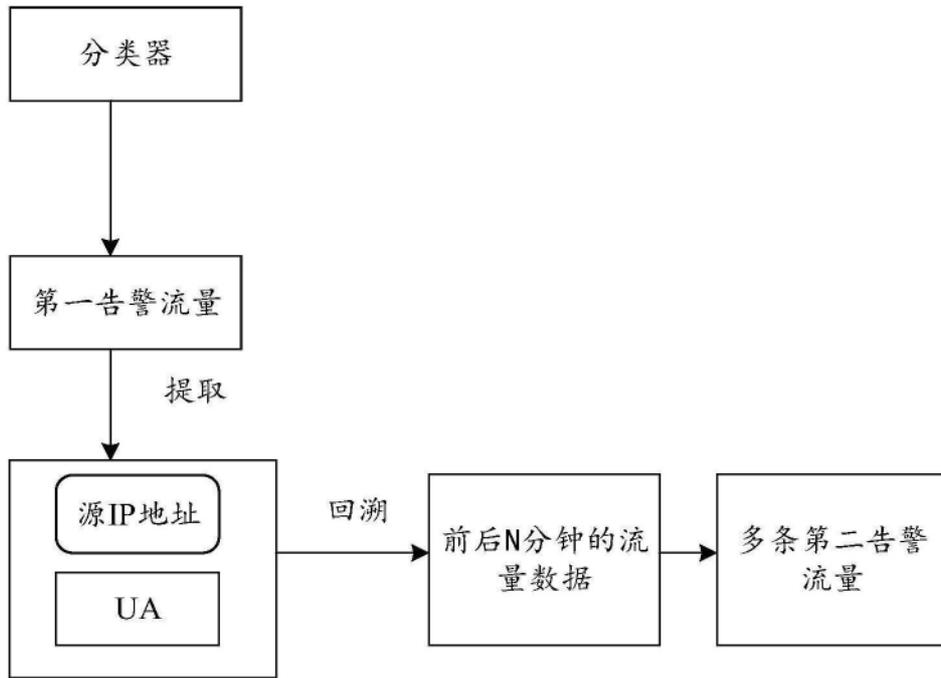


图5

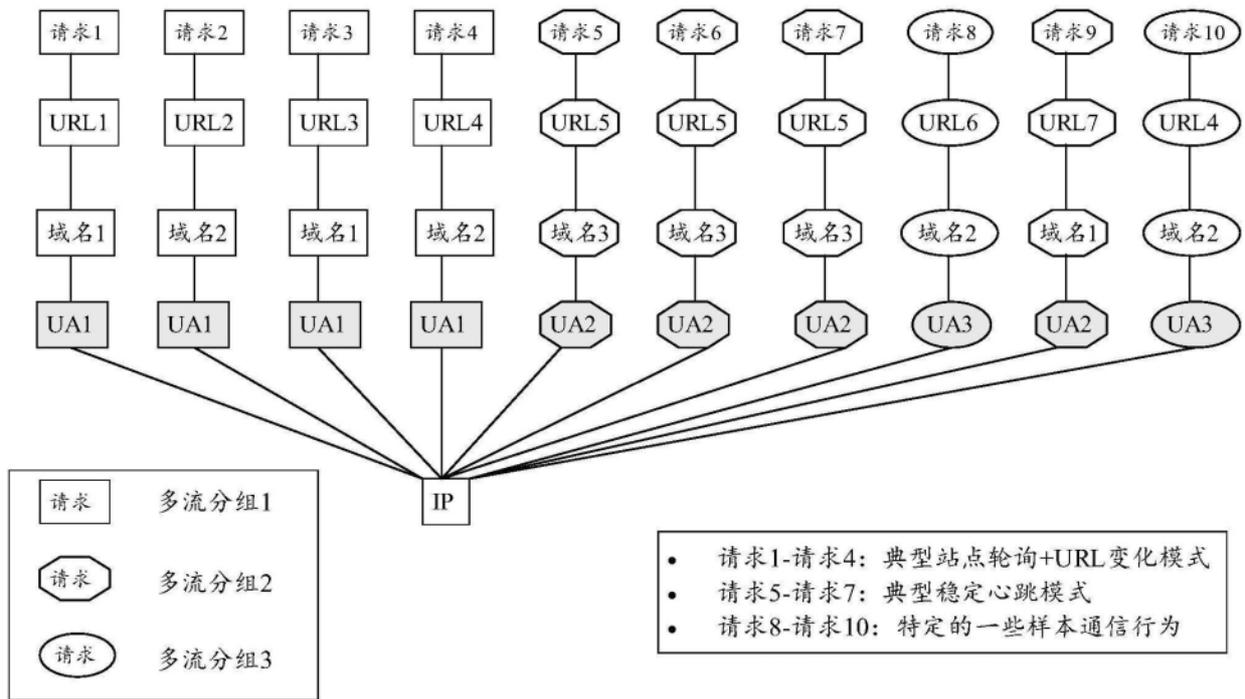


图6

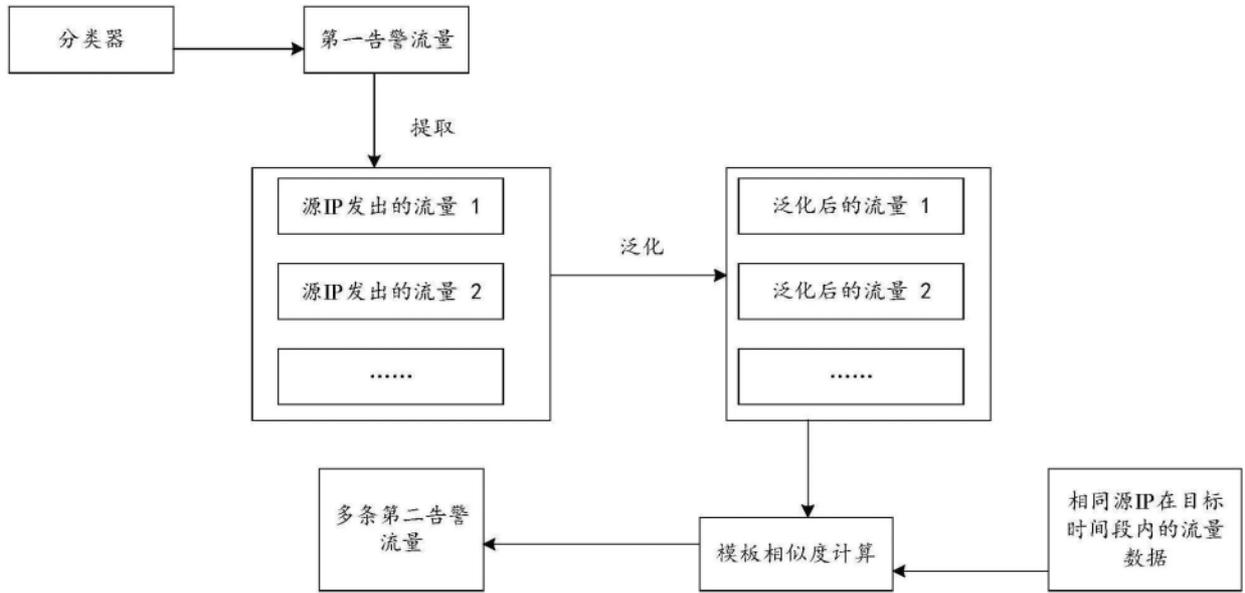


图7

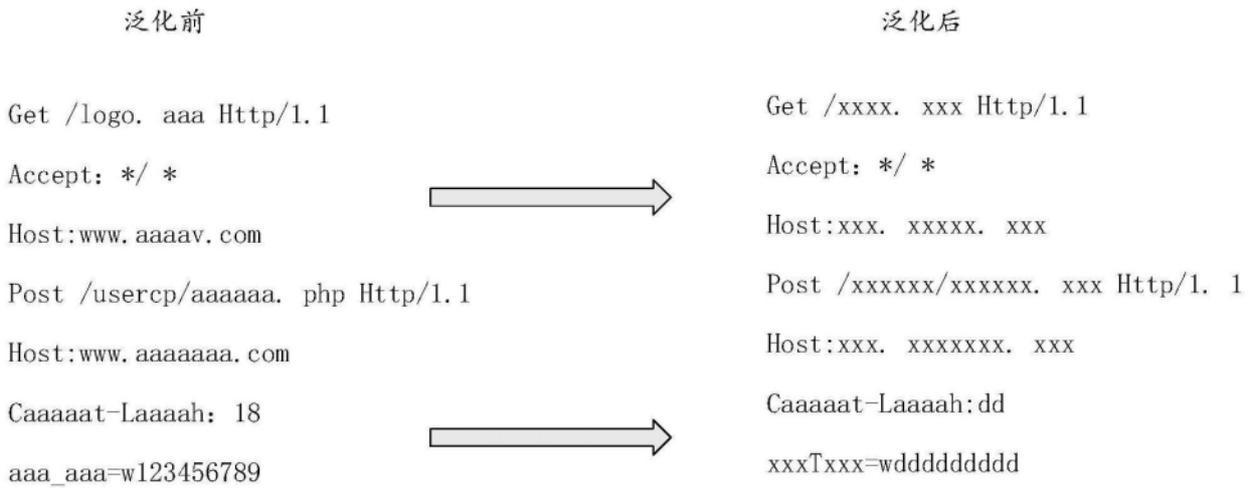


图8

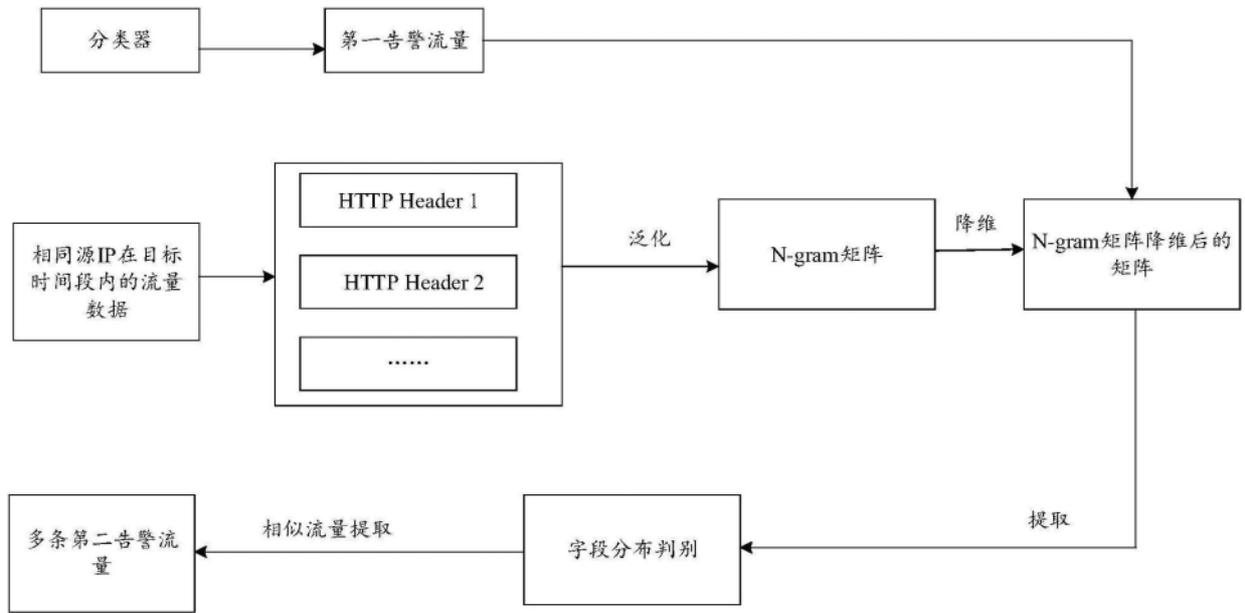


图9

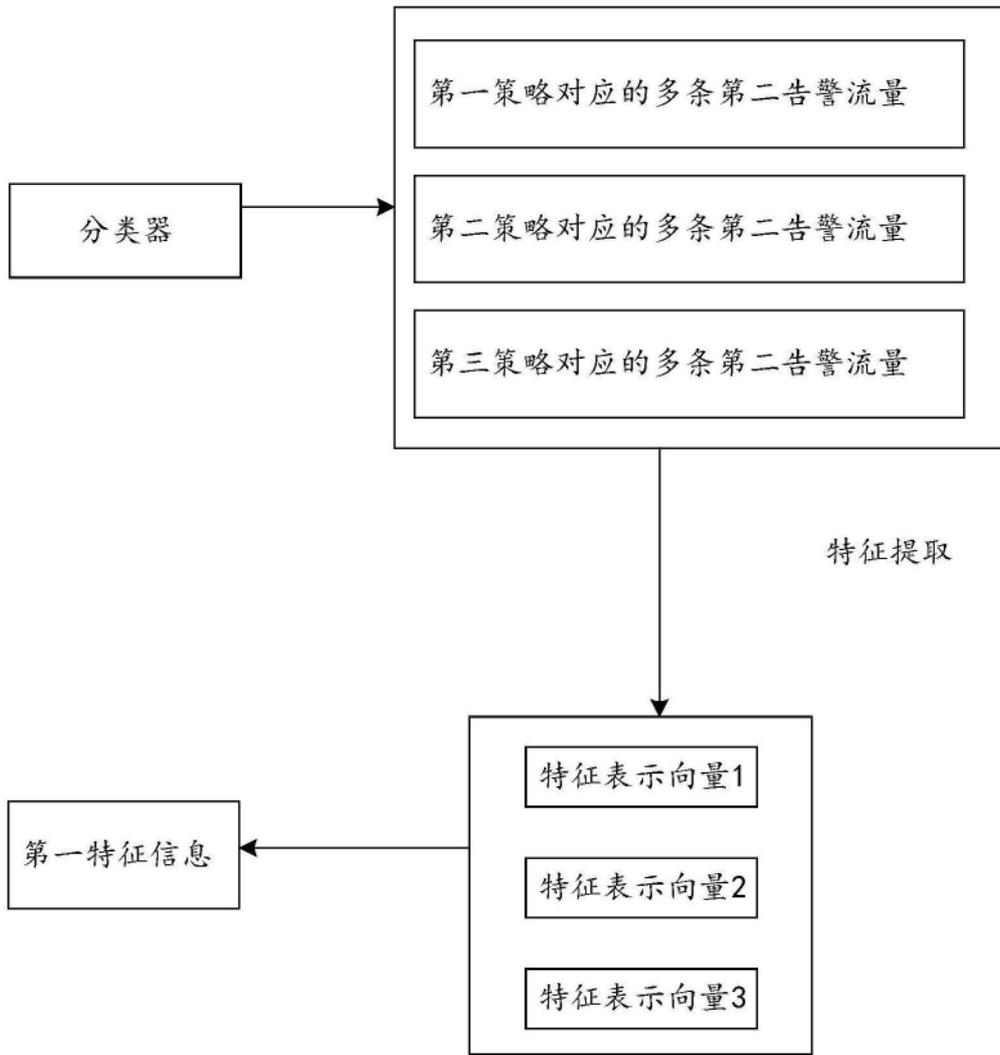


图10

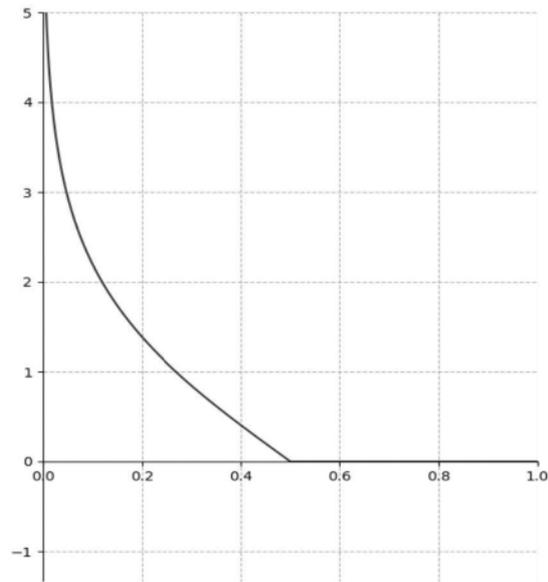


图11

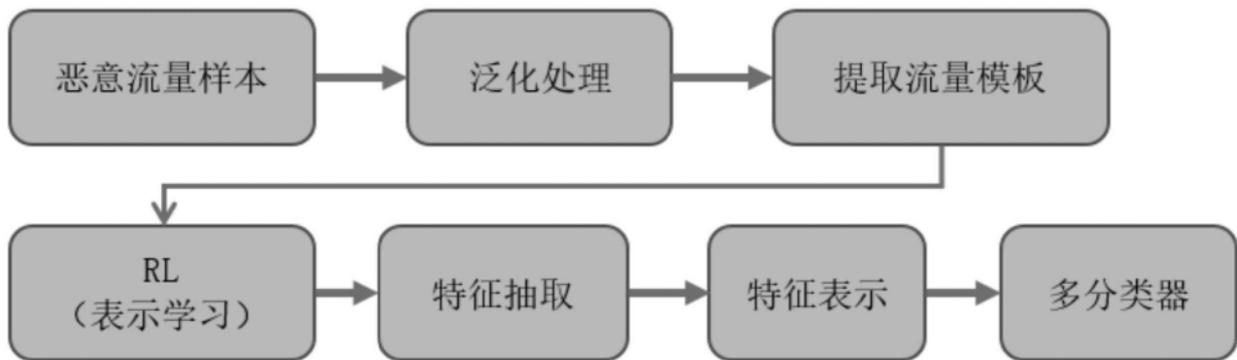


图12

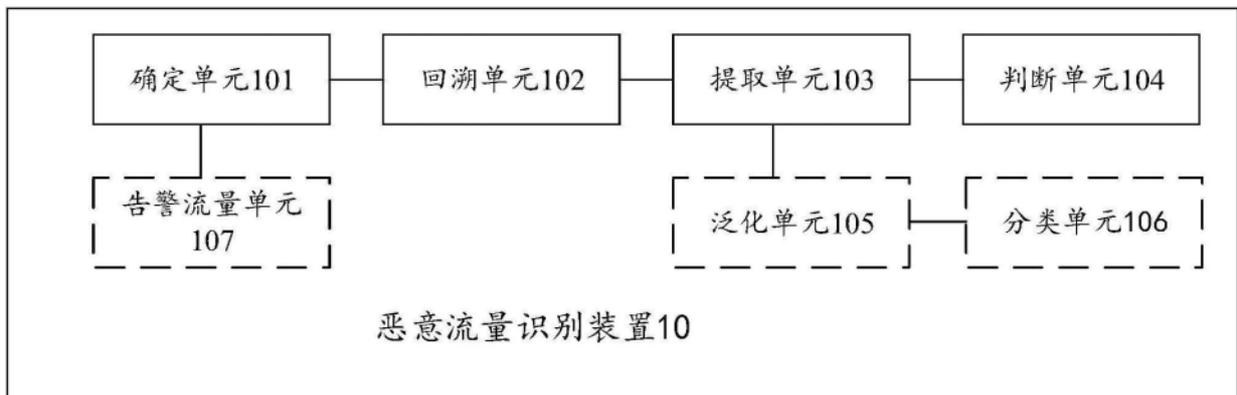


图13

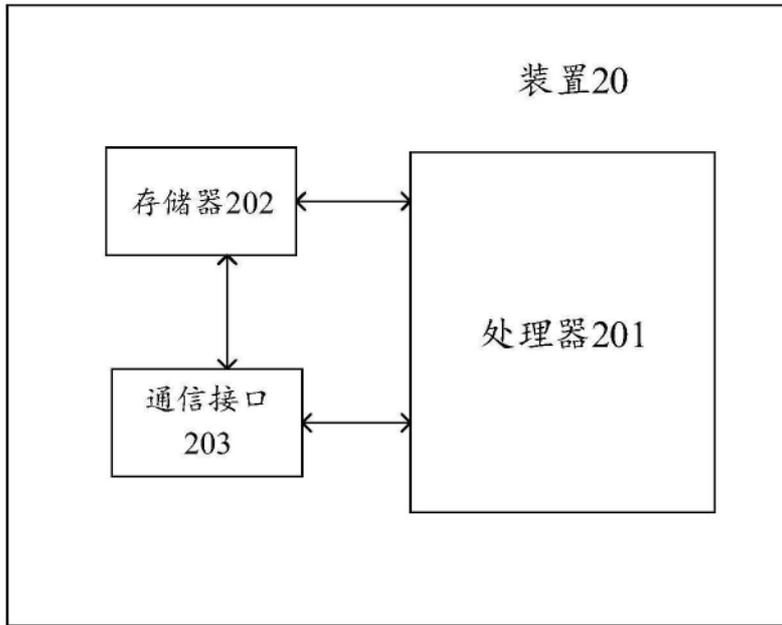


图14