(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104463635 A
(43)申请公布日 2015.03.25

(21)申请号 201410806896.2

(22)申请日 2014.12.22

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 李纪峰 杨毅

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
G06Q 30/02(2012.01)

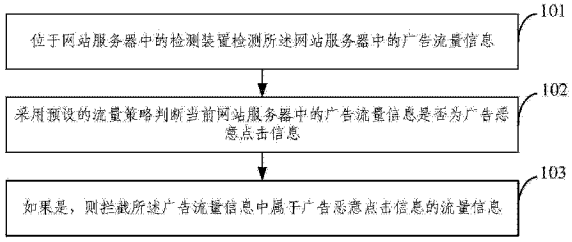
权利要求书2页 说明书8页 附图2页

(54)发明名称

广告恶意点击检测方法及装置

(57)摘要

本发明公开了一种广告恶意点击检测方法及装置，该方法包括：位于网站服务器侧的检测装置检测所述网站服务器中的广告流量信息；采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；如果是，则拦截所述广告流量信息中属于广告恶意点击信息的流量信息。该方法通过位于网站服务器中的检测装置检测所述网站服务器中的广告流量信息，并通过预设的流量策略判断该广告流量信息是否为广告恶意点击信息，在该广告流量信息为恶意信息时，将属于广告恶意点击信息的信息进行拦截，该方法通过对广告恶意点击行为的检测和拦截，防止了广告恶意点击的计费，保护了广告商的利益，提高了网络广告的投放效果。



CN 104463635 A

1. 一种广告恶意点击检测装置，其特征在于，包括：

检测模块，用于检测网站服务器中的广告流量信息；

判断模块，用于采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

第一拦截模块，用于在所述判断模块判断当前网站服务器中的广告流量信息为广告恶意点击信息时，拦截所述广告流量信息中属于广告恶意点击信息的流量信息。

2. 根据权利要求 1 所述的装置，其特征在于，所述广告流量信息包括下述的一项或多项：

所述广告的信息、点击所述广告的 IP 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

3. 根据权利要求 1 所述的装置，其特征在于，所述装置还包括：

接收模块，用于在所述检测模块检测所述网站服务器中的广告流量信息之前，接收服务器发送的流量策略；

所述服务器中的流量策略为所述服务器根据多个检测装置上报的广告恶意点击信息统计的策略。

4. 根据权利要求 1 所述的装置，其特征在于，所述装置还包括：

负向概率确定模块，用于在判断模块判断当前网站服务器中的广告流量信息不属于广告恶意点击信息之后，采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为该广告流量信息属于广告恶意点击信息的概率；

第二拦截模块，用于在所述负向概率符合预设范围时，将所述负向概率对应的广告流量信息进行拦截。

5. 根据权利要求 4 所述的装置，其特征在于，所述装置还包括：

发送模块，用于将所述广告流量信息中属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器。

6. 一种广告恶意点击检测方法，其特征在于，包括：

位于网站服务器侧的检测装置检测所述网站服务器中的广告流量信息；

采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

如果是，则拦截所述广告流量信息中属于广告恶意点击信息的流量信息。

7. 根据权利要求 6 所述的方法，其特征在于，所述广告流量信息包括下述的一项或多项：

所述广告的信息、点击所述广告的 IP 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

8. 根据权利要求 6 所述的方法，其特征在于，所述流量策略为所述检测装置在检测所述网站服务器中的广告流量信息之前接收服务器发送的流量策略；

所述服务器中的流量策略为所述服务器根据多个检测装置上报的广告恶意点击信息统计的策略。

9. 根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

在采用预设的流量策略判断当前网站服务器中的广告流量信息不属于广告恶意点击

信息之后，采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为该广告流量信息属于广告恶意点击信息的概率；

如果所述负向概率符合预设范围，则将所述负向概率对应的广告流量信息进行拦截。

10. 根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

所述广告流量信息中将属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器。

广告恶意点击检测方法及装置

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及一种广告恶意点击检测方法及装置。

背景技术

[0002] 随着互联网的普及和信息技术的飞速发展，网络广告正以超越传统媒体广告的速度飞速发展。在传统媒体广告中，比如电视广告，收视率是体现广告播放效果的一种有效形式。在网络广告播放中，除了利用某个广告的曝光量来体现该广告的播放效果外，越来越多的广告客户希望能了解到底有多少用户对这个广告感兴趣。一般的，如果用户对这个广告感兴趣，那么用户会点击该广告，从而产生网络点击事件，在某段事件内，用户在浏览到web页面中的网络广告以后，点击该广告，打开广告链接页面，这个过程为一个有效的网络点击。

[0003] 网络广告主在搜索引擎投放推广的广告之后，每个上网用户基本上都可以收到网络广告，互联网搜索引擎会根据用户的点击行为对广告主进行收费。这种计费方法在搜索引擎广告推广中普遍使用。而上网用户群体复杂，除了存在点击广告的正常行为之外，还有一些恶意点击的行为。比如，有些黑客通过编写相关程序实现恶意点击，有些利益体，比如竞争对手恶意点击，人为的增加广告的点击次数，造成广告商家支付大量的无效广告的费用。

[0004] 这种恶意点击一方面会严重损害商家的利益，并伤害了商家对点击付费以及该模式的搜索引擎运营商的信任；另一方面，广告商家对搜索引擎的不信任造成了他们不愿意在此广告方式上的投入，直接影响了搜索引擎公司的盈利。

[0005] 因此，如何较好的防止网络广告被恶意点击，减少网络广告的开销，提高网络广告的投放效果成为了一种需求。

发明内容

[0006] 针对现有技术中的缺陷，本发明提供了一种广告恶意点击检测方法及装置，实现了对广告恶意点击行为的检测和拦截，防止广告恶意点击的计费，提高了网络广告的投放效果。

[0007] 第一方面，本发明提供一种广告恶意点击检测装置，包括：

[0008] 检测模块，用于检测网站服务器中的广告流量信息；

[0009] 判断模块，用于采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

[0010] 第一拦截模块，用于在所述判断模块判断当前网站服务器中的广告流量信息为广告恶意点击信息时，拦截所述广告流量信息中属于广告恶意点击信息的流量信息。

[0011] 可选地，所述广告流量信息包括下述的一项或多项：

[0012] 所述广告的信息、点击所述广告的IP地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

[0013] 可选地，所述装置还包括：

[0014] 接收模块，用于在所述检测模块检测所述网站服务器中的广告流量信息之前，接收服务器发送的流量策略；

[0015] 所述服务器中的流量策略为所述服务器根据多个检测装置上报的广告恶意点击信息统计的策略。

[0016] 可选地，所述装置还包括：

[0017] 负向概率确定模块，用于在判断模块判断当前网站服务器中的广告流量信息不属于广告恶意点击信息之后，采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为该广告流量信息属于广告恶意点击信息的概率；

[0018] 第二拦截模块，用于在所述负向概率符合预设范围时，将所述负向概率对应的广告流量信息进行拦截。

[0019] 可选地，所述装置还包括：

[0020] 发送模块，用于将所述广告流量信息中属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器。

[0021] 第二方面，本发明还提供了一种广告恶意点击检测方法，包括：

[0022] 位于网站服务器侧的检测装置检测所述网站服务器中的广告流量信息；

[0023] 采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

[0024] 如果是，则拦截所述广告流量信息中属于广告恶意点击信息的流量信息。

[0025] 可选地，所述广告流量信息包括下述的一项或多项：

[0026] 所述广告的信息、点击所述广告的 IP 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

[0027] 可选地，所述流量策略为所述检测装置在检测所述网站服务器中的广告流量信息之前接收服务器发送的流量策略；

[0028] 所述服务器中的流量策略为所述服务器根据多个检测装置上报的广告恶意点击信息统计的策略。

[0029] 可选地，所述方法还包括：

[0030] 在采用预设的流量策略判断当前网站服务器中的广告流量信息不属于广告恶意点击信息之后，采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为该广告流量信息属于广告恶意点击信息的概率；

[0031] 如果所述负向概率符合预设范围，则将所述负向概率对应的广告流量信息进行拦截。

[0032] 可选地，所述方法还包括：

[0033] 所述广告流量信息中将属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器。

[0034] 由上述技术方案可知，本发明提供的一种广告恶意点击检测方法及装置，该方法通过检测所述网站服务器中的广告流量信息，并通过预设的流量策略判断该广告流量信息是否为广告恶意点击信息，在该广告流量信息为恶意信息时，将属于广告恶意点击信息的信息进行拦截，该方法通过对广告恶意点击行为的检测和拦截，防止了广告恶意点击的计

费，保护了广告商的利益，提高了网络广告的投放效果。

附图说明

[0035] 图 1 为本发明一实施例提供的广告恶意点击检测方法的流程示意图；

[0036] 图 2 为本发明另一实施例提供的广告恶意点击检测方法的流程示意图；

[0037] 图 3 为本发明一实施例提供的广告恶意点击检测装置的结构示意图。

具体实施方式

[0038] 下面结合附图，对发明的具体实施方式作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案，而不能以此来限制本发明的保护范围。

[0039] 图 1 示出了本发明实施例提供的广告恶意点击检测方法，如图 1 所示，该广告恶意点击检测方法具体包括如下步骤：

[0040] 101、位于网站服务器中的检测装置检测所述网站服务器中的广告流量信息；

[0041] 上述网站服务器可以由第三方软件公司的服务器中的检测装置来执行，也可以由投放广告商的服务器中的检测装置来执行。

[0042] 上述广告流量信息至少包括下述一种：所述广告的信息、点击所述广告的互联网协议 (Internet Protocol，简称 IP) 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间等。本实施例仅对广告流量信息进行举例说明，该广告流量信息还可包括其他信息，本实施例不对其进行限定

[0043] 102、采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

[0044] 本实施例中的预设的流量策略为所述检测装置在检测所述网站服务器中的广告流量信息之前可接收服务器发送的流量策略。

[0045] 其中，所述服务器中的流量策略为所述服务器根据多个检测装置上报的广告恶意点击信息统计的策略。

[0046] 上述服务器可以为云端服务器。也就是说所有网站服务器侧的检测装置可连接云端服务器，在实时监控网站服务器中的广告流量信息的过程中可实时接收云服务器下载或更新的流量策略，以便保证较为准确的检测网站服务器的广告流量信息中的广告恶意点击信息。

[0047] 上述广告恶意点击信息为通过上述预设的流量策略进行判断的。

[0048] 举例来说，流量策略可为：黑名单 IP 地址 and在预设时间段内点击广告次数 and 点击广告逗留时间等。

[0049] 或者，流量策略可为：黑名单 IP 地址 and在预设时间段内点击广告次数 or点击广告逗留时间等，本实施例仅对流量策略进行举例说明，可根据实际需要和实际的广告信息确定针对该广告流量信息的流量策略。

[0050] 103、如果是，则拦截广告流量信息中属于广告恶意点击信息的流量信息。

[0051] 也就是说，将所述广告流量信息中属于广告恶意点击信息的信息进行拦截。

[0052] 当然，如果上述步骤 102 中采用流量策略判断当前网站服务器中的广告流量信息不属于广告恶意点击信息时，可放行当前检测的广告流量信息。

[0053] 可以理解的是，在上述步骤 102 之后，当采用预设的流量策略判断出该广告流量信息为广告恶意点击信息时，则将该广告流量信息的信息进行拦截，以阻止网站服务器对该广告恶意点击进行收费。

[0054] 上述方法通过根据云端服务器下发的流量策略对网站服务器中的广告流量信息进行检测，从而识别出哪些为广告恶意点击信息，并对检测出的广告恶意点击信息进行拦截防止广告恶意点击收费，该方法相对于现有技术对于已付费的广告恶意点击收费进行识别和过滤，拦截准确，效率高。

[0055] 图 2 示出了本发明实施例提供的广告恶意点击检测方法，如图 2 所示，该广告恶意点击检测方法具体包括如下步骤：

[0056] 201、位于网站服务器侧的检测装置检测所述网站服务器中的广告流量信息；

[0057] 上述广告流量信息至少包括下述一种：所述广告的信息、点击所述广告的 IP 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

[0058] 举例来说，该广告信息中包括该广告的信息标识，通过该标识可以获知该广告的广告商、该广告的内容、该广告的对应的搜索引擎运营商等与该广告相关的一些信息。

[0059] 202、采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息。

[0060] 通常，流量策略中可包括最近时间段内的针对该广告信息的 IP 黑名单，或者，流量策略还可包括最近时间段内每一 IP 针对该广告信息的平均点击次数范围等。

[0061] 需要说明的是，上述预设的流量策略为预先接收云端服务器发送的流量策略；其中，云端服务器中的流量策略为根据多个检测装置上报的广告恶意点击信息统计的策略。

[0062] 上述广告恶意点击信息为通过上述预设的流量策略进行判断的。

[0063] 上述流量策略可以根据上述广告流量信息的内容进行制定，具体的，假设检测解析广告流量信息，进而根据解析的信息与流量策略进行匹配，以确定是否在流量策略的范围内，如果在，则确定属于广告恶意点击信息。广告流量信息的解析举例如下：所述广告的信息 A、点击所述广告的 IP 地址 B、点击所述广告的时间点信息 C、在预设时间段内点击所述广告的次数 D、每次点击所述广告逗留的时间 E 等；

[0064] 举例来说，上述解析广告流量信息的可以对如下分类，比如上述假设点击该广告的 IP 包括与该广告信息不相关的 IP 地址 B1、与该广告竞争对手的 IP 地址 B2 等；点击该广告的时间点的信息可以包括 7:00-9:00 时间段为 C1、9:00-18:00 时间段为 C2、18:00-23:00 时间段为 C3、23:00-7:00 时间段为 C4 四个时段；在预设时间段内点击所述广告的次数可以包括：在小于 5 秒钟内点击不小于 3 次 D1、在不小于 5 秒钟且小于 5 分钟内点击不小于 1 次 D2、在不小于 5 秒钟且小于 5 分钟内点击不小于 10 次 D3、不小于 5 分钟点击 1 次 D4；点击该广告逗留的时间可以包括小于 5 秒 E1、不小于 5 秒钟且小于 5 分钟 E2、不小于 5 分钟 E3 等。

[0065] 上述解析广告流量信息的分类本实施例仅用于举例说明，并不对其进行限定。

[0066] 例如上述预设时间段内点击所述广告的次数，可以理解为点击该广告的同一 IP 在预设时间段内点击所述广告的次数。该预设时间段可以以小时为单位，或者以分钟为单位。如果以分钟为单位，则该预设时间段可以理解为 5 分钟内同一 IP 点击该广告的次数等

等

[0067] 如表 1 所示，本实施例中可以根据上述广告流量信息以及对广告流量信息进行解析后，并根据实际情况设定针对该广告的流量策略。

[0068] 表 1 ：

[0069]

广告流量信息	广告流量信息特征分类
广告的信息A	--
点击广告的IP地址B	与该广告信息不相关的IP地址B1、 与该广告竞争对手的IP地址B2
点击广告的时间点信息C	7:00-9:00时间段C1、 9:00-18:00时间段C2、 18:00-23:00时间段C3、 23:00-7:00时间段C4
在预设时间段内点击广告的次数D	小于5秒钟内点击不小于3次D1、 在不小于5秒钟且小于5分钟内点击不小于1次D2、 在不小于5秒钟且小于5分钟内点击不小于10次D3、 不小于5分钟点击1次D4
每次点击广告逗留的时间E	小于5秒E1、 不小于5秒钟且小于5分钟E2、 不小于5分钟E3

[0070] 上述流量策略可以这样进行设定，对存在 B2orC4orD1orD2orE1 时的广告流量信息的信息进行拦截或丢弃；或对存在 B1and(C1orC2orC3orC4)andD1orE1 时的广告流量信息的信息进行拦截或丢弃；对 B1and(C1orC2orC3orC4)andD4orE3 的广告流量信息的信息不进行拦截或丢弃，且对其进行放行，以使搜索引擎运营公司对该电机进行收费；对 B1and(C1orC2orC3orC4)andD2orE2 的广告流量信息的信息不进行拦截或丢弃，且将该广告流量信息进行待检测，不对其进行放行。本实施例中的上述策略仅用于举例说明，不对上述流量策略的具体排列方式进行具体限定。

[0071] 203、如果是，则将所述广告流量信息中属于广告恶意点击信息的信息进行拦截。

[0072] 可以理解的是，当采用预设的流量策略判断当前网站服务器中的广告流量信息为广告恶意点击信息，既满足上述 B2orC4orD1orD2orE1 或 B1and(C1orC2orC3orC4)

andD1orE1 时，则认为该广告流量信息为广告恶意点击信息。

[0073] 在具体应用中，比如说在遇到上述对于 B1and(C1orC2orC3orC4)andD2orE2 的广告流量信息时，即与该广告竞争对手 IP 不同的 IP 点击该广告信息时，且在某一时间段内在不小于 5 秒钟且小于 5 分钟内点击不小于 1 次，且该点击的逗留时间小于 5 秒，则可以认为该广告点击可能某个 IP 地址的用户在点击之前对该广告感兴趣，且看到该广告之后发现该广告并不是他想要的；另一种情况是还可以认为该广告点击可能为广告恶意点击，但是为了避开拦截，故意避开预设的策略。上述两种情况下，并不能够直观判断该广告点击是否为广告恶意点击，因此，此时为了更加精准的将广告流量信息中为广告恶意点击信息概率较大的广告流量信息识别出来，本实施例的上述方法还包括如下检测步骤，具体的上述方法还包括如下步骤：

[0074] 204、在步骤 202 中在采用预设的流量策略判断当前网站服务器中的广告流量信息不属于广告恶意点击信息之后，则采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为属于广告恶意点击信息的概率；

[0075] 本实施例中的预设算法可以为在预先训练的贝叶斯模型中查找的与该广告流量信息的匹配度，并获取该广告流量信息的正向权重值的正向概率和负向权重值的负向概率。

[0076] 举例来说，如果包含在预设时间段内在不小于 5 秒钟且小于 5 分钟内点击该广告的次数不小于 1 次，在上述模型中与该特征相同的有 100 条信息，其中，与该特征相同的且属于广告恶意点击信息的有 80 条，与该特征相同的且属于非广告恶意点击信息的有 20 条，则认为该广告流量信息对应的正向权重值为 0.8，负向权重值为 0.2。

[0077] 上述方法适用于对采用预设的流量策略判断当前网站服务器中的广告流量信息不属于广告恶意点击信息时，再通过上述预设算法进行计算该广告流量信息属于广告恶意点击信息的概率。故上述方法还包括以下步骤：

[0078] 205、判断上述负向概率是否符合预设范围；

[0079] 206、如果所述负向概率符合所述预设范围，则将所述负向概率对应的广告流量信息的信息进行拦截或丢弃。

[0080] 举例来说，若负向概率的预设范围为 0.5 ～ 0.9，则计算 B1and(C1orC2orC3orC4)andD2orE2 的广告流量信息的概率为 0.8，则将该广告流量信息的信息进行拦截或丢弃。

[0081] 207、如果所述负向概率不符合预设范围，则将所述负向概率对应的广告流量信息的信息放行。

[0082] 在另一个可能实现的方式中，若负向概率的预设范围为 0.5 ～ 0.9，，则计算 B1and(C1orC2orC3orC4)andD2orE2 的广告流量信息的负向概率为 0.45，则将该负向概率对应的广告流量信息的信息放行。

[0083] 为了使上述步骤 202 中的流量策略为最新的流量策略，故上述方法还包括下述步骤 208：

[0084] 208、所述广告流量信息中将属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送云端服务器。

[0085] 在具体应用中，通过检测装置将属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器，实现了对上述云端服务器中的流量策略进行更

新，该策略的更新可以实时的也可以定时的，例如每天更新一次等。

[0086] 图 3 示出了本发明实施例提供的一种广告恶意点击检测装置，如图 3 所示，该装置包括：检测模块 31、判断模块 32 和第一拦截模块 33。

[0087] 检测模块 31，用于检测网站服务器中的广告流量信息；

[0088] 具体的，广告流量信息包括：所述广告的信息、点击所述广告的 IP 地址、点击所述广告的时间点信息、在预设时间段内点击所述广告的次数、每次点击所述广告逗留的时间。

[0089] 判断模块 32，用于采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息；

[0090] 第一拦截模块 33，用于在所述判断模块判断当前网站服务器中的广告流量信息为广告恶意点击信息时，拦截所述广告流量信息中属于广告恶意点击信息的流量信息。

[0091] 具体的，上述装置还包括图 3 中未示出的接收模块 34。

[0092] 接收模块 34，用于在所述流量策略为所述检测模块在检测所述网站服务器中的广告流量信息之前，接收服务器发送的流量策略；

[0093] 所述服务器中的流量策略为所述服务器根据多个检测模块上报的广告恶意点击信息统计的策略。

[0094] 在采用上述流量策略不能够直观判断该广告点击是否为广告恶意点击时，为了更加精准的将广告流量信息中为广告恶意点击信息负向概率较大的广告流量信息识别出来，上述装置还包括图中未示出的负向概率确定模块 35 和第二拦截模块 36；

[0095] 该负向概率确定模块 35，用于在判断模块判断当前网站服务器中的广告流量信息不属于广告恶意点击信息之后，采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为该广告流量信息属于广告恶意点击信息的概率；

[0096] 第二拦截模块 36，用于在所述负向概率符合预设范围时，将所述负向概率对应的广告流量信息进行拦截。

[0097] 为了对上述云端服务器中的流量策略进行更新，上述装置还包括图中未示出的发送模块 37：

[0098] 发送模块 37，用于将所述广告流量信息中属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送服务器。

[0099] 上述装置与上述方法是一一对应的，上述方法的详细例子说明也同样适用于该装置，本发明不对上述装置的实施细节进行详细说明。

[0100] 本发明的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0101] 类似地，应当理解，为了精简本发明公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释呈反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0102] 本领域技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在于该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是互相排斥之处，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0103] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0104] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的一种浏览器终端的设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0105] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0106] 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，其均应涵盖在本发明的权利要求和说明书的范围当中。

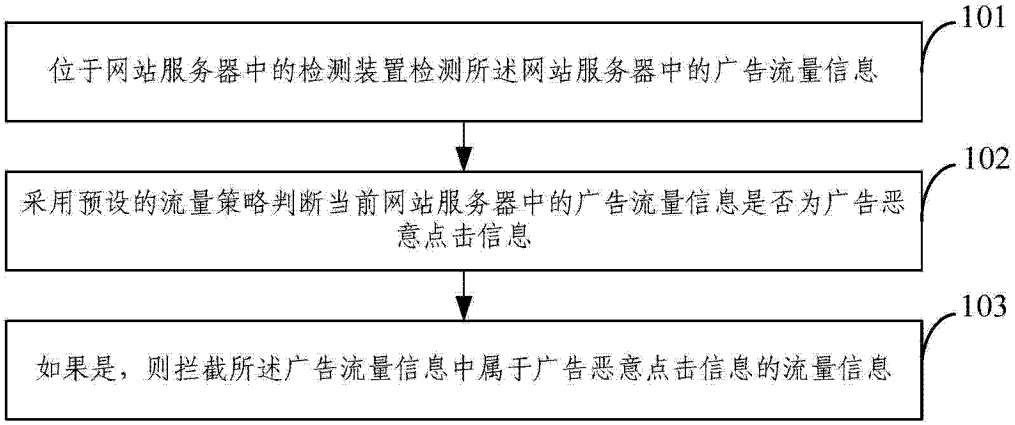

位于网站服务器中的检测装置检测所述网站服务器中的广告流量信息
101
采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息
102
如果是，则拦截所述广告流量信息中属于广告恶意点击信息的流量信息
103

图 1

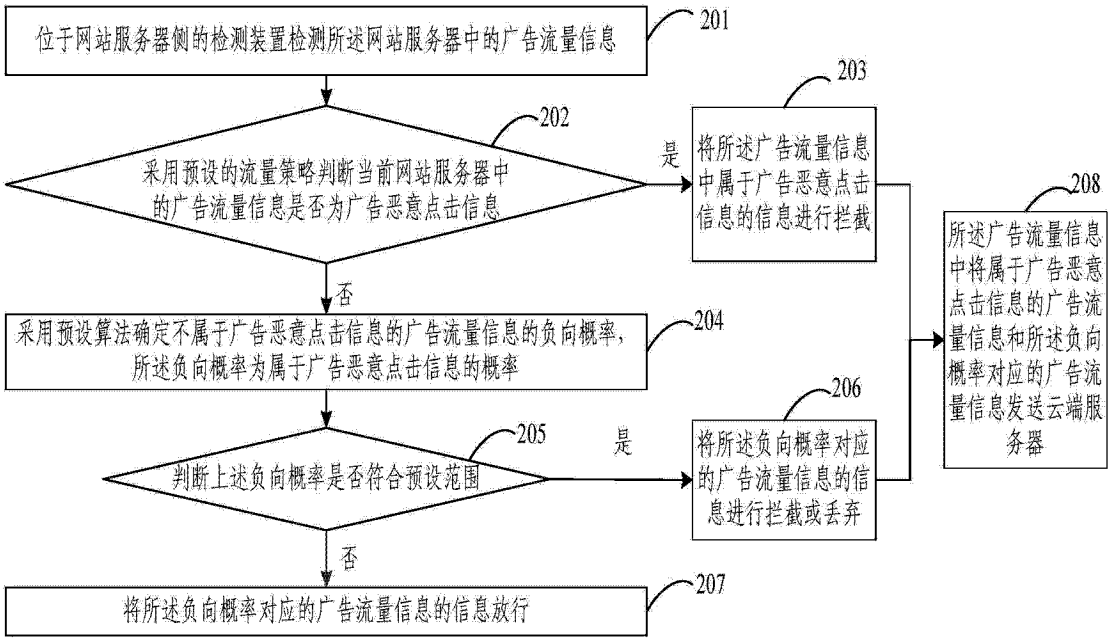

位于网站服务器侧的检测装置检测所述网站服务器中的广告流量信息
201
采用预设的流量策略判断当前网站服务器中的广告流量信息是否为广告恶意点击信息
202
是
否
将所述广告流量信息中属于广告恶意点击信息的信息进行拦截
203
采用预设算法确定不属于广告恶意点击信息的广告流量信息的负向概率，所述负向概率为属于广告恶意点击信息的概率
204
判断上述负向概率是否符合预设范围
205
是
否
将所述负向概率对应的广告流量信息的信息进行拦截或丢弃
206
将所述负向概率对应的广告流量信息的信息放行
207
所述广告流量信息中将属于广告恶意点击信息的广告流量信息和所述负向概率对应的广告流量信息发送云端服务器
208

图 2

图 3