(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 102739683 B
(45)授权公告日 2015.09.09

(21)申请号 201210226566.7
(22)申请日 2012.06.29
(73)专利权人 杭州迪普科技有限公司
地址 310000 浙江省杭州市滨江区通和路68号中财大厦6层
(72)发明人 李鑫
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
(56)对比文件
CN 101789940 A,2010.07.28, 说明书第53段-第65段.
CN 101572701 A,2009.11.04, 全文.
US 2007204040 A1,2007.08.30, 全文.
CN 102185723 A,2011.09.14, 说明书第28段-第33段,权利要求1-5.
审查员 徐佳

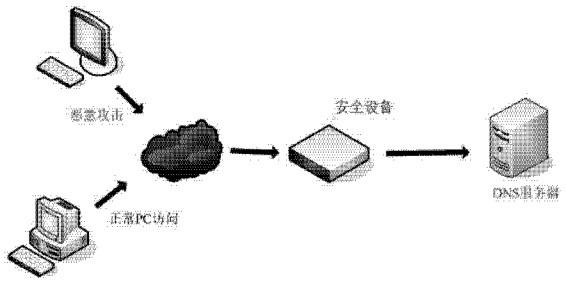
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种网络攻击过滤方法及装置

(57)摘要

本发明提供一种网络攻击过滤方法,应用于安全设备上,为DNS服务器提供网络攻击过滤的服务,该方法包括:A、在收到用户的DNS请求报文时判断是否为首次发送,如果否,转步骤B处理,否则丢弃该报文并将该DNS会话信息以及用户行为参数作为保存到DNS会话表中;B、从DNS会话表中获取与当前DNS请求报文携带的会话信息对应的用户行为参数,并判断当前报文携带的用户行为参数与DNS会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准,如果是则合法,否则丢弃该报文。本发明用户协议栈上的行为特点,有效地过滤了对于DNS服务器的攻击。



CN 102739683 B

1. 一种网络攻击过滤装置，应用于安全设备上，为 DNS 服务器提供网络攻击过滤的服务，该装置包括报文区分单元以及行为分析单元，其特征在于：

报文区分单元，用于在收到用户的 DNS 请求报文时判断 DNS 请求报文携带的 DNS 会话信息在 DNS 会话表中是否有相应的记录，如果是，则提交行为分析单元进行处理，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文，并将该 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存到 DNS 会话表中，其中所述 DNS 会话信息至少包括目的域名以及源 IP 地址；

行为分析单元，用于从 DNS 会话表中获取与当前 DNS 请求报文携带的会话信息对应的用户行为参数，并判断当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准，如果是则确定该 DNS 请求报文合法，否则确定该 DNS 请求报文不合法，并丢弃该 DNS 请求报文；

其中，所述用户行为参数为 DNS 请求报文的接收时间和 / 或 DNS 请求报文携带的 IP ID；所述正常用户行为标准相应为当前 DNS 请求报文的接收时间与 DNS 会话表中记录的接收时间的差值在预设的范围内，和 / 或当前 DNS 请求报文携带的 IP ID 与 DNS 会话表中记录的 IP ID 不相同。

2. 如权利要求 1 所述的装置，其特征在于，所述 DNS 会话信息进一步包括 DNS 请求报文的目的 IP 地址。

3. 如权利要求 1 所述的装置，其特征在于，所述行为分析单元用于在确定当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异符合正常用户行为标准时，进一步判断当前 DNS 请求报文的重传次数是否达到预设的阈值，如果是则确定该 DNS 请求报文合法，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文。

4. 如权利要求 3 所述的装置，其特征在于，所述预设的阈值大于或者等于 2。

5. 一种网络攻击过滤方法，应用于安全设备上，为 DNS 服务器提供网络攻击过滤的服务，其特征在于，该方法包括：

A、在收到用户的 DNS 请求报文时判断 DNS 请求报文携带的 DNS 会话信息在 DNS 会话表中是否有相应的记录，如果是，转步骤 B 处理，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文，并将该 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存到 DNS 会话表中，其中所述 DNS 会话信息至少包括目的域名以及源 IP 地址；

B、从 DNS 会话表中获取与当前 DNS 请求报文携带的会话信息对应的用户行为参数，并判断当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准，如果是则确定该 DNS 请求报文合法，否则确定该 DNS 请求报文不合法，并丢弃该 DNS 请求报文；

其中，所述用户行为参数为 DNS 请求报文的接收时间和 / 或 DNS 请求报文携带的 IP ID；所述正常用户行为标准相应为当前 DNS 请求报文的接收时间与 DNS 会话表中记录的接收时间的差值在预设的范围内，和 / 或当前 DNS 请求报文携带的 IP ID 与 DNS 会话表中记录的 IP ID 不相同。

6. 如权利要求 5 所述的方法，其特征在于，所述 DNS 会话信息进一步包括 DNS 请求报文的目的 IP 地址。

7. 如权利要求 5 所述的方法，其特征在于，所述步骤 B 进一步包括：在确定当前 DNS 请

求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异符合正常用户行为标准时，进一步判断当前 DNS 请求报文的重传次数是否达到预设的阈值，如果是则确定该 DNS 请求报文合法，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文。

8. 如权利要求 7 所述的方法，其特征在于，所述预设的阈值大于或者等于 2。

一种网络攻击过滤方法及装置

技术领域

[0001] 本发明涉及网络安全技术，尤其涉及一种应用于安全设备上保护 DNS 服务器的网络攻击过滤方法及装置。

背景技术

[0002] 人们的工作和生活正在从不断进步的网络技术上受益，然而随着网络规模的迅速扩大，网络安全问题变得日益严峻。网络上的各种攻击行为层出不穷，DoS（Denial of Service 拒绝服务）攻击就是其中最为典型的网络攻击行为。DDoS（分布式拒绝服务）攻击自从 2000 年首次出现后，DDoS 攻击事件每天都在发生，而且呈现出越演越烈的状态。许多个人用户和各类企业网络遭受到 DDoS 攻击。DDos 攻击可导致网络拥塞、服务器或其他主机停止处理用户请求、企业网站瘫痪、企业网络不能工作等问题。这些问题严重影响人们的生活和社会的工作。

[0003] 攻击者往往会选择网络中的关键节点展开攻击，比如针对 DNS 服务器进行攻击。因为 DNS 服务器较容易接触，恶意攻击者易于发起针对 DNS 服务器的 DDoS 攻击。然而 DNS 服务器又很重要，一旦 DNS 服务器被攻击，可能会导致整个区域网络不可用，甚至因为 DNS 的递归查询方式导致整个 DNS 服务群瘫痪，因此保证 DNS 服务器的安全尤为重要。

[0004] 现有的 DNS 服务器防 DDoS 攻击的方案通常是在被保护 DNS 服务器前增加检测防护设备（以下简称安全设备），安全设备的工作机制包括：

[0005] 机制 A：实时检测每个用户的 DNS 请求数，当检测到某用户 DNS 请求报文数量超过设定的每个用户请求的正常阀值，则判定 DNS 服务器遭受到该用户攻击，此时启动针对该用户的限速防护策略，把该用户流量限制到可接受范围，从而保护 DNS 服务器。

[0006] 机制 B：实时检测 DNS 请求报文的总数量，当检测到 DNS 请求报文的总数量超过设定的正常阀值，则判定 DNS 服务器可能遭受到分布式拒绝服务攻击，此时启动总的限速防护策略，把总流量限制 DNS 服务器可承受范围，从而保护 DNS 服务器。

[0007] 机制 A 需要监测每个用户的 DNS 请求报文的数量，即需要维护每个用户的请求报文数量的统计，当面对成千上万的用户时维护的难度成倍增加。而且恶意攻击者可能伪装成正常用户，发出大量伪装 DNS 请求报文，此时限速机制可能导致该正常用户无法正常使用网络。而且如果恶意攻击者采用分布式，离散性的攻击方式导致机制 A 无法区分正常访问和恶意访问，只能通过机制 B 进行总体限速，然而机制 B 的限速手段会导致正常访问用户也受到限速影响。

[0008] 此外，无论是机制 A 还是机制 B，都存在检测可能不及时的问题，当攻击呈现出突发与大量特点时，虽然可以被安全设备检测到，但由于检测可能存在滞后性，大量恶意攻击流量可能在这段检测滞后的时间段越过安全设备访问了 DNS 服务器，而 DNS 服务器也很可能因为瞬间大量突发攻击流量而瘫痪，安全设备的保护失去了意义。如何确保 DNS 设备免受 DDoS 攻击并尽可能地将对用户正常访问的影响降到最低，是目前安全设备提供商迫切需要解决的问题。

发明内容

[0009] 本发明提供一种网络攻击过滤装置，应用于安全设备上，为 DNS 服务器提供网络攻击过滤的服务，该装置包括报文区分单元以及行为分析单元，其中：

[0010] 报文区分单元，用于在收到用户的 DNS 请求报文时判断 DNS 请求报文携带的 DNS 会话信息在 DNS 会话表中是否有相应的记录，如果是，则提交行为分析单元进行处理，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文，并将该 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存到 DNS 会话表中，其中所述 DNS 会话信息至少包括目的域名以及源 IP 地址；

[0011] 行为分析单元，用于从 DNS 会话表中获取与当前 DNS 请求报文携带的会话信息对应的用户行为参数，并判断当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准，如果是则确定该 DNS 请求报文合法，否则确定该 DNS 请求报文不合法，并丢弃该 DNS 请求报文。

[0012] 本发明还提供一种网络攻击过滤方法，应用于安全设备上，为 DNS 服务器提供网络攻击过滤的服务，该方法包括：

[0013] A、在收到用户的 DNS 请求报文时判断 DNS 请求报文携带的 DNS 会话信息在 DNS 会话表中是否有相应的记录，如果是，转步骤 B 处理，否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文，并将该 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存到 DNS 会话表中，其中所述 DNS 会话信息至少包括目的域名以及源 IP 地址；

[0014] B、从 DNS 会话表中获取与当前 DNS 请求报文携带的会话信息对应的用户行为参数，并判断当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准，如果是则确定该 DNS 请求报文合法，否则确定该 DNS 请求报文不合法，并丢弃该 DNS 请求报文。

[0015] 本发明巧妙地利用了 DNS 流程中用户协议栈上的行为特点，有效地过滤了对于 DNS 服务器的攻击，对于 DDoS 这样的攻击过滤效果显著，并且对于用户上网体验的影响非常轻微，难以被感知到。

附图说明

[0016] 图 1 是本发明一种实施方式中网络攻击过滤装置的逻辑结构图。

[0017] 图 2 是本发明一种典型的组网示意图。

[0018] 图 3 是本发明一种实施方式网络攻击过滤方法的处理流程图。

具体实施方式

[0019] 本发明为 DNS 服务器提供一种精确的网络攻击过滤方法及装置，其设计原理不再像现有技术那样从报文数量以及速率着手进行粗犷式地防护，而是从用户对 DNS 服务器正常访问的行为特点着手，甄别出用户正常的访问与恶意攻击。请参考图 1，以计算机程序实现为例（本发明并不排除其他实现方式），本发明一种网络攻击过滤装置应用于安全设备上，为 DNS 服务器提供网络攻击过滤的服务，该装置包括：报文区分单元以及行为分析单元。安全设备可以采用流行的硬件架构，其主要包括 CPU、内存、存储器以及包括业务插卡在

内的各种业务硬件(并不是必须的)。在一种基础性的实施方式中,请参考图 2 以及图 3,所述网络攻击过滤装置运行时主要包括以下步骤 :

[0020] 步骤 101,报文区分单元收到用户的 DNS 请求报文,判断 DNS 请求报文携带的 DNS 会话信息在 DNS 会话表中是否有相应的记录,如果是,则转步骤 102 提交行为分析单元进行处理,否则丢弃该 DNS 请求报文以促使用户重传该 DNS 请求报文,并将该 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存到 DNS 会话表中,其中所述 DNS 会话信息至少包括目的域名以及源 IP 地址。

[0021] 步骤 102,行为分析单元从 DNS 会话表中获取与当前 DNS 请求报文携带的会话信息对应的用户行为参数,并判断当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异是否符合正常用户行为标准,如果是则确定该 DNS 请求报文合法,否则确定该 DNS 请求报文不合法,并丢弃该 DNS 请求报文。

[0022] 在本发明中,首先需要从 DNS 请求这个应用维度来记录每个用户的 DNS 会话信息。DNS 会话信息用来唯一标识一个 DNS 会话,DNS 会话是一种应用级的会话,通常对应表示用户(比如某个 IP 地址)针对一个特定域名(比如 Sina)的 DNS 请求。如果用户针对 Sina 进行第一次域名解析失败,比如 DNS 请求报文因为各种原因在传输过程中被丢弃了,通常用户操作系统的协议栈会在预设的时间内重新发送 DNS 请求报文,如果第二次 DNS 请求依然没有成功,那么协议栈会进行再次重新发送 DNS 请求报文。每次重新发送的时间间隔可能并不一样,比如 XP 系统中第一次重传的时间间隔大约为 1 秒,而第二次重传与第一次重传的时间间隔则会提高到大约 2 秒。不同的操作系统,重传的时间间隔的设计上可能略有差异,但这种差异并不影响本发明的具体实现。由于攻击者往往是通过构造 DNS 请求报文进行攻击的,攻击者并不会像正常用户的协议栈那样等待数秒的时间对 DNS 请求报文进行重传,首先攻击者的主机无法承受这样的处理压力,而且等待这么长的时间,攻击已经显然会失去意义。在一种较佳的实施方式中,本发明正是利用用户这种正常重传行为来过滤攻击者构造的攻击报文。

[0023] 请参考表 1 的示例,假设用户(192.168.1.2)首次发送 DNS 请求向 DNS 服务器(10.10.1.25)请求解析 Sina 的 IP 地址,其发送的 DNS 请求报文会被安全设备收到,上送到报文区分单元进行处理,报文区分单元提取 DNS 请求报文携带的 DNS 会话信息(比如报文的源 IP 地址以及目的域名)去匹配 DNS 会话表(初始为空),由于用户是首次请求解析 Sina 的 IP 地址,不会匹配到任何一条对应的记录。报文区分单元将该报文携带 DNS 会话信息以及对应的报文接收时间作为一条新的记录保存到 DNS 会话表中,并将该 DNS 请求报文丢弃。在优选的实施方式中,DNS 会话信息还可以进一步包括目的 IP 地址和 / 或 TTL 值。在少数情况中,用户可能会向不同的 DNS 服务器(比如说主备两个 DNS 服务器)发送 DNS 请求报文,这两个请求显然属于不同的会话,因为会话的对象不一样了。因此可以引入报文的目的 IP 地址到 DNS 会话信息中,这样 DNS 会话信息对 DNS 会话的标识将更加精确。当然为了,更加精确地标识,还可以引入 TTL 值,因为大部分的操作系统的协议栈在重传 DNS 请求报文时都会使用相同的 TTL 值。

[0024]

源 IP 地址	目的 IP 地址	目的域名	TTL	IP ID	接收时间	重传次数

192.168.1.5	10.10.1.25	Google	a	123	X	1
192.168.1.6	10.10.1.25	Baidu	b	254	Y	2
192.168.1.7	10.10.1.25	Sina	c	584	Z	1
.....	.....	.....	.....	.....	.....	.....

[0025] 表 1

[0026] 由于用户首次发送的 DNS 请求报文被丢弃，用户操作系统的协议栈会在等待预定的时间间隔后进行 DNS 请求报文第一次重传。由于 DNS 请求报文的 DNS 会话信息已经被保存到 DNS 会话列表中。报文区分单元收到重传的 DNS 请求报文，会从报文中提取到与首次 DNS 请求报文同样 DNS 会话信息，因而查找 DNS 会话表会命中一条记录，此时需要转步骤 102 提交行为分析单元进行处理。

[0027] 行为分析单元获取 DNS 会话表中与 DNS 会话信息对应的报文接收时间(也就是上次 DNS 请求报文的接收时间)，然后将当前 DNS 请求报文的接收时间与获取的报文接收时间进行对比，如果两者的差值符合预设的重传时间间隔标准，那么当前的 DNS 请求报文可以确定为合法的 DNS 请求报文，否则确定为攻击报文。以 XP 系统为例，假设 XP 系统的重传间隔为 1 秒，那么接收用户首次发送的 DNS 请求报文到接收到用户重传 DNS 请求报文的时间间隔必然大于等于 1 秒，考虑到网络延迟的因素，这个时间间隔可能会大于 1S，因此可以根据实际情况预设一个正常的重传时间间隔标准，比如说大于 1 秒小于等于 1.5 秒这样一个范围。如果行为分析单元分析后发现时间间隔不再上述范围中，则说明当前 DNS 请求报文并不是用户正常重传的 DNS 请求报文，多数是攻击者仿冒用户发送的 DNS 请求报文，于是可以确定当前 DNS 请求报文的是不合法的，并将该报文丢弃。

[0028] 在上述的实施方式中，是以报文接收时间作为用户行为参数进行示例说明的。在另一实施方式中，还可以使用 DNS 请求报文携带的 IP ID 作为用户行为参数。DNS 请求报文是一个 IP 报文，正常用户的协议栈每发送一个 IP 报文均会将 IP ID 加 1，这样一来对于安全设备来说，收到一个重传的 DNS 请求报文，其 IP ID 必然与前一次收到的 DNS 请求报文的 IP ID 不同。而攻击者往往并不是按照正常协议栈去处理报文的 IP ID 的，因为那样太浪费攻击者的计算机处理资源，因此攻击报文的 IP ID 很多时候都是相同的。在本实施方式中，可以选用 IP ID 作为用户行为参数来使用。行为分析单元可以比较重传的 DNS 请求报文 IP ID 与 DNS 会话表中记录的 IP ID 之间的差异，如果两者相同，则可以确定当前 DNS 请求报文是不合法的，如果不同，则可以确定为合法的。

[0029] 在优选的实施方式中，报文接收时间以及 IP ID 除了可以单独使用，还可以结合使用，行为分析单元只有确定 IP ID 的差异以及报文接收时间的差异均符合对应的正常用户行为标准时才确定当前 DNS 请求报文是合法的，否则确定为非法的。将两个用户行为参数一起使用，可以让攻击者仿冒用户发送攻击报文的难度变得更大。即便其知晓了本发明这样的防范机制也难以实施攻击。因为本发明会故意将 DNS 会话中的首次发送的 DNS 请求报文丢弃，攻击者要想绕过本发明的过滤机制，必须要使得自己的行为与正常用户的行为一样，按照协议栈的正常流程去走，而攻击者往往是大量发送报文，每个报文都按照协议栈

的正常流程再进行一次重传，这将需要巨大的计算资源，而且每两个报文中只有一个报文能通过，相当攻击效率下降了 50%。需要说明的是，虽然本发明也要求合法用户重传 DNS 请求报文，但事实上对用户上网体验影响很小，难以被感知到，因为用户可能在首次访问 Sina 时需要多等待 1 秒(因为 DNS 请求需要重传)，一旦 DNS 请求被 DNS 服务器应答之后，用户获得 Sina 的 IP 地址之后就会在本地形成 DNS 缓存，用户再次访问 Sina 则不需要进行解析，因为用户本地的 DNS 缓存会保存 Sina 与其 IP 地址的对应关系，只要用户不清空本地的 DNS 缓存，下次访问 Sina 时，并不需要发送 DNS 请求报文来解析 Sina 的 IP 地址了。

[0030] 进一步来说，为了进一步提高本发明的过滤机制安全等级，可以要求用户进行多次重传。行为分析单元在确定当前 DNS 请求报文携带的用户行为参数与 DNS 会话表中记录的用户行为参数之间的差异符合正常用户行为标准时，进一步判断 DNS 会话表中对应的重传次数(初始均为 0)是否达到预设的重传阈值，如果是则确定当前 DNS 请求报文合法，否则将该 DNS 请求报文丢弃，并将重传次数加 1。假设预设的重传阈值是 2，则意味着正常用户需要重传两次才能通过行为分析单元的合法性检查。同样的道理，由于用户操作系统有 DNS 缓存机制，所以对于用户的影响仅仅是首次访问一个网站时等待需要等待 3-4 秒，这样的时间通常是可以被容忍的，其影响是轻微的。然而对于攻击者的攻击而言，对正常用户的协议栈的模拟要非常彻底，这要消耗极其巨大的计算资源，攻击难度大幅度提高。即便攻击者能够获得这样的计算资源，假设重传阈值为 2，那就意味着攻击者发送 3 个报文才有 1 个能通过，攻击效率又大幅度降低。本发明巧妙地利用了 DNS 流程中用户协议栈上的行为特点，有效地过滤了对于 DNS 服务器的攻击，对于 DDoS 这样的攻击过滤效果显著，并且对于用户上网体验的影响非常轻微，难以被感知到。

[0031] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

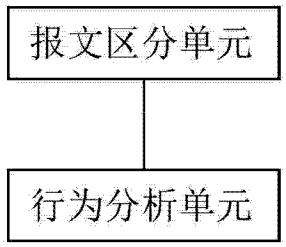


图 1

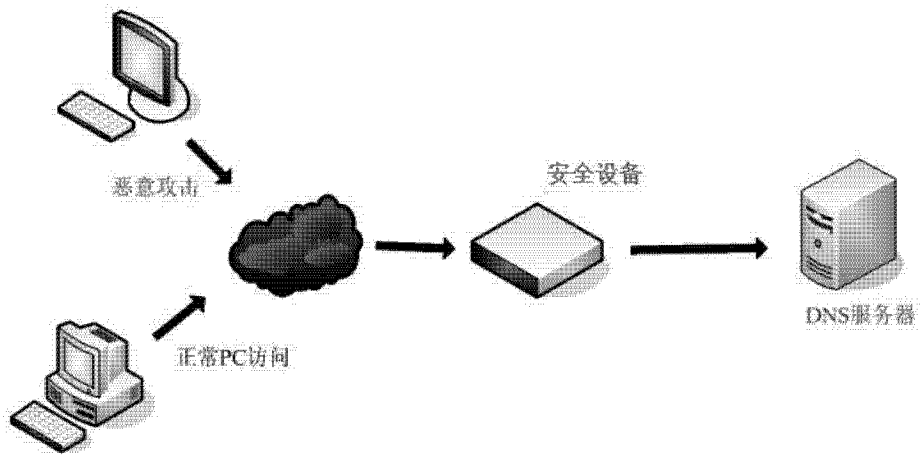


图 2

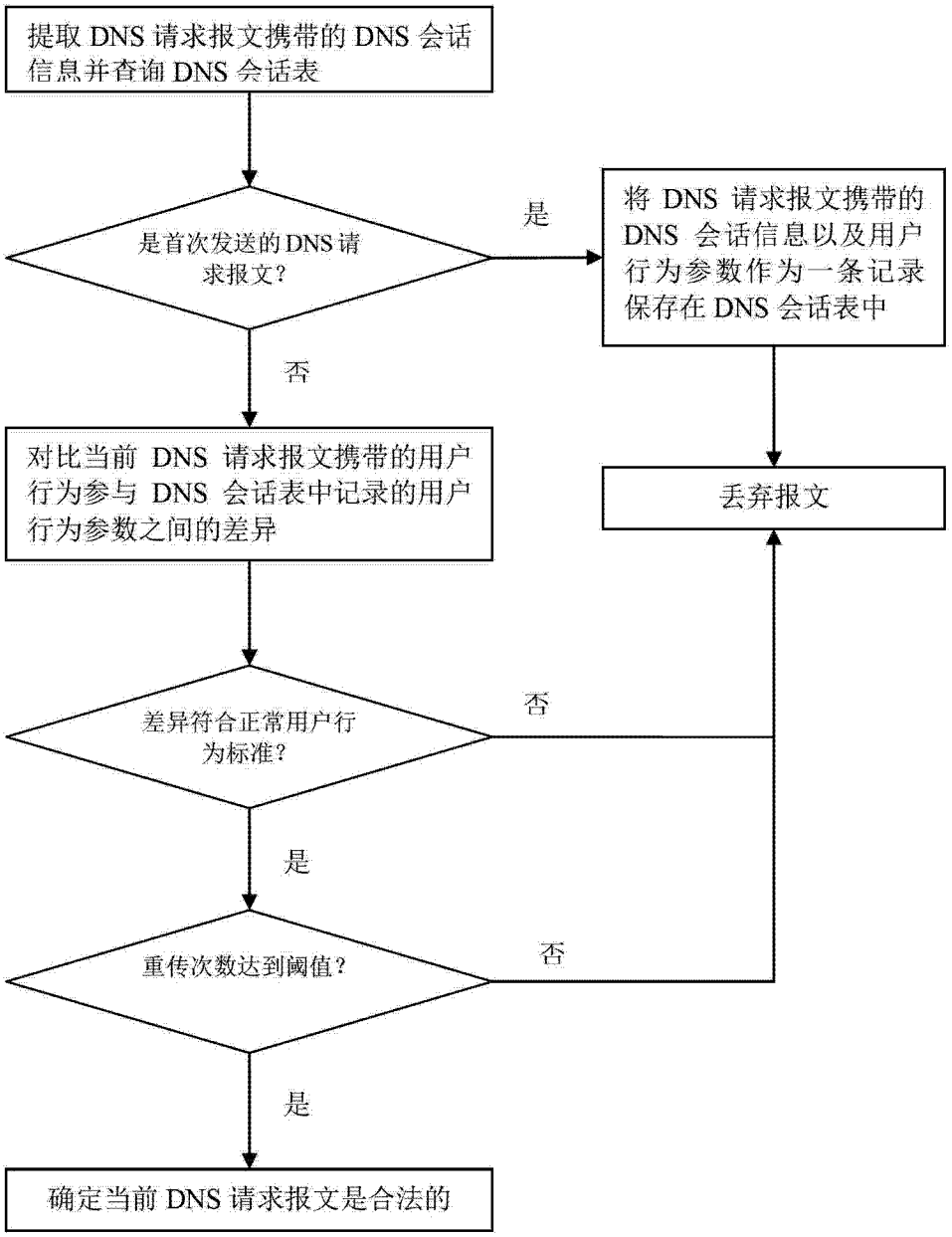

提取 DNS 请求报文携带的 DNS 会话信息并查询 DNS 会话表
是首次发送的 DNS 请求报文？
是
将 DNS 请求报文携带的 DNS 会话信息以及用户行为参数作为一条记录保存在 DNS 会话表中
否
对比当前 DNS 请求报文携带的用户行为参与 DNS 会话表中记录的用户行为参数之间的差异
丢弃报文
差异符合正常用户行为标准？
否
是
重传次数达到阈值？
否
是
确定当前 DNS 请求报文是合法的

图 3