[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780040606.6

[43] 公开日 2009 年 9 月 16 日

[11] 公开号 CN 101536455A

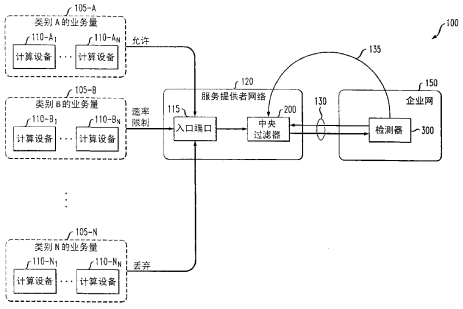
[22] 申请日 2007.10.23
[21] 申请号 200780040606.6
[30] 优先权
[32] 2006.11.3 [33] US [31] 11/592，726
[86] 国际申请 PCT/US2007/022446 2007.10.23
[87] 国际公布 WO2008/063344 英 2008.5.29
[85] 进入国家阶段日期 2009.4.30
[71] 申请人 朗讯科技公司
地址 美国新泽西州
[72] 发明人 迈克尔·巴里·格林沃德
埃里克·亨利·格罗塞
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王波波
权利要求书 2 页 说明书 19 页 附图 6 页

[54] 发明名称

用于在一个或多个分组网络中恶意攻击期间递送控制消息的方法和设备

[57] 摘要

提供了如下的方法和设备：用于例如在恶意攻击期间，在一个或多个分组网络中向中央过滤器可靠地递送控制消息，而不需要中央过滤器对检测器进行响应或肯定应答。 目标受害者使用检测器、通过如下方式来防御不期望业务量：基于对从一个或多个源 IP 地址接收到的分组的分析，确定目标受害者接收到不期望业务量；以及将通告废除消息发送到与服务提供者相关联的中央过滤器，该通告废除消息用于识别至少一个源计算设备的源地址，其中，该至少一个源计算设备向目标受害者的分组发送将要经受以下一个或多个：限制、丢弃、或允许，并且，使用无需来自中央过滤器的即时肯定应答的通告废除协议来发送通告废除消息。 此外，可以向中央过滤器冗余地发送通告废除消息，且优选地，通告废除消息是自持的。



1、一种用于由目标受害者防御不期望业务量的方法，所述目标受害者具有一个或多个目的地地址，所述方法包括以下步骤：

基于对从一个或多个源 IP 地址接收到的分组的分析，确定所述目标受害者接收到不期望业务量；以及

将通告废除消息发送到与服务提供者相关联的中央过滤器，所述通告废除消息用于识别至少一个源计算设备的源地址，其中，所述至少一个源计算设备向所述目标受害者的分组发送将要经受以下一个或多个：限制、丢弃、或允许，并且，使用无需来自所述中央过滤器的即时肯定应答的通告废除协议来发送所述通告废除消息。

2、根据权利要求 1 所述的方法，其中，所述不期望业务量包括恶意攻击或拒绝服务攻击。

3、根据权利要求 1 所述的方法，其中，将所述通告废除消息冗余地发送到所述中央过滤器。

4、根据权利要求 1 所述的方法，其中，所述通告废除消息是自持的。

5、根据权利要求 1 所述的方法，其中，所述通告废除协议提供粗时钟同步。

6、根据权利要求 1 所述的方法，还包括以下步骤：接收来自所述中央过滤器的共享状态以及维护对所述状态的任何改变。

7、根据权利要求 1 所述的方法，其中，所述通告废除协议包括一个或多个特征以避免针对所述通告废除协议的恶意攻击。

8、根据权利要求 1 所述的方法，其中，所述通告废除消息包括允许以下一个或多个操作的序列号：调解来自多个所述目标受害者的冲突通告废除消息；避免针对所述通告废除协议的恶意攻击；以及丢弃所述通告废除消息的副本。

9、一种用于由目标受害者防御不期望业务量的设备，所述目标受害者具有一个或多个目的地地址，所述设备包括：

存储器；以及

至少一个处理器，耦合至存储器，所述至少一个处理器用于：

基于对从一个或多个源 IP 地址接收到的分组的分析，确定所述目标受害者接收到不期望业务量；以及

将通告废除消息发送到与服务提供者相关联的中央过滤器，所述通告废除消息用于识别至少一个源计算设备的源地址，其中，所述至少一个源计算设备向所述目标受害者的分组发送将要经受以下一个或多个：限制、丢弃、或允许，并且，使用无需来自所述中央过滤器的即时肯定应答的通告废除协议来发送所述通告废除消息。

10、根据权利要求 9 所述的设备，其中，将所述通告废除消息冗余地发送到所述中央过滤器。

用于在一个或多个分组网络中恶意攻击期间递送控制消息的方法和设备

相关申请的交叉引用

本申请涉及名称为“Method and Apparatus for Defending Against Denial of Service Attacks in IP Networks by Target Victim Self-Identification and Control”的美国专利申请11/197,842以及名称为“Method and Apparatus for Defending Against Denial of Service Attacks in IP Networks Based on Specified Source/Destination IP Address Pairs”的美国专利申请11/197,841，这两个专利申请均于2005年8月5日提交，均被转让给本发明的受让人且并入此处以供参考。

技术领域

本发明涉及针对基于分组的通信网络的计算机安全技术，更具体地涉及用于在这种基于分组的网络中检测并通告废除不期望的业务量，例如拒绝服务攻击或另一恶意攻击。

背景技术

诸如拒绝服务（DoS）攻击之类的恶意攻击试图使得计算机资源对于其预期用户不可用。例如，对web服务器的DoS攻击常常导致所主持的网页不可用。当需要将有限的资源分配给攻击者而不是合法用户时，DoS攻击可以导致显著的服务中断。发起攻击的机器通常通过在互联网上发送大量的互联网协议（IP）分组，来造成针对攻击目标受害者的损害。例如，DoS攻击可以包括：试图“泛滥”网络，从而阻止合法网络业务量；或试图通过发送比服务器能够处理的更多的请求来中断服务器，从而阻止对一个或多个服务的访问。

已提出或建议了多种用于防御这种恶意攻击的技术。例如，名称为“Method and Apparatus for Defending Against Denial of Service

Attacks in IP Networks by Target Victim Self-Identification and Control”的美国专利申请11/197,842以及名称为“Method and Apparatus for Defending Against Denial of Service Attacks in IP Networks Based on Specified Source/Destination IP Address Pairs”的美国专利申请11/197,841公开了用于检测并通告废除DoS攻击的技术。

防御这种恶意攻击的系统通常采用与客户网络相关联的检测器以及服务提供者的网络中的中央过滤器，以保护客户网络免于恶意攻击。通常，检测器将检测对客户网络的恶意攻击并向中央过滤器发送一个或多个通告废除或通知消息。例如，在确定了恶意攻击正在进犯客户网络时，检测器可以向中央过滤器发送一个或多个源/目的地IP地址对，该中央过滤器使服务提供者限制源IP地址和目的地IP地址与任意所发送的源/目的地IP地址对的源IP地址和目的地IP地址相匹配的那些IP分组的发送，从而限制（或消除）恶意攻击。检测器通常位于靠近客户网络的位置。

然而，恶意攻击通常导致大量分组丢失，使得很可能丢失或长时间延迟从中央过滤器到检测器的控制消息。此外，在恶意攻击期间，检测器很可能繁忙并处于沉重的负担下。防御这种恶意攻击的现有系统通常采用传输层安全（TLS）、安全套接字层（SSL）、安全命令解释程序（SSH）或其他基于传输控制协议（TCP）的协议，它们要求针对向中央过滤器发送控制消息的肯定应答。除了在恶意攻击期间以外，这样的信道通常是足够的。在恶意攻击期间，检测器可能无法收到来自中央过滤器的肯定应答，或者该肯定应答可能在检测器的输入缓冲器超载时到达检测器。通常，检测器不能继续处理，直到中央过滤器适当地肯定应答了所有在前的通告废除消息。

因此，需要如下的方法和设备：用于在一个或多个分组网络中恶意攻击期间向中央过滤器可靠地递送控制消息，而不需要中央过滤器对检测器进行响应。

发明内容

总体上，提供了如下的方法和设备：用于例如在恶意攻击期间，在一个或多个分组网络中向中央过滤器可靠地递送控制消息，而不需要中央过滤器对检测器进行响应或肯定应答。根据本发明的一个方面，目标受害者使用检测器、通过如下方式来防御不期望业务量：基于对从一个或多个源IP地址接收到的分组的分析，确定目标受害者接收到不期望业务量；以及将通告废除消息发送到与服务提供者相关联的中央过滤器，该通告废除消息用于识别至少一个源计算设备的源地址，其中，该至少一个源计算设备向目标受害者的分组发送将要经受以下一个或多个：限制、丢弃、或允许，并且，使用无需来自中央过滤器的即时肯定应答的通告废除协议来发送通告废除消息。

根据本发明的另一方面，可以向中央过滤器冗余地发送通告废除消息，且优选地，通告废除消息是自持的（self contained）。中央过滤器和检测器共享状态信息，并可选地维护对状态信息的任何改变。

根据本发明的另一方面，所公开的通告废除协议包括一个或多个特征以避免针对通告废除协议自身的恶意攻击。例如，可选地，通告废除消息包括如下序列号：（i）允许调解来自多个所述目标受害者的冲突通告废除消息；（ii）允许避免针对通告废除协议的恶意攻击；以及（iii）允许丢弃通告废除消息的副本。

通过参考以下详细说明以及附图，将会对本发明以及本发明的其他特征和优点有更完整的理解。

附图说明

图1示出了本发明可操作的网络环境；

图2是图1所示的中央过滤器系统的示意框图；

图3是图1所示的检测器的示意框图；

图4和图5是描述了并入本发明特征的拒绝服务过滤过程的示例性实现方式的流程图；

图6示出了针对UDP分组预先考虑的、用于UDP请求的HMAC密钥；以及

图7示出了DP记录报头和报尾在安全可靠流内的示例性布局。

具体实施方式

本发明提供用于在一个或多个分组网络中恶意攻击期间向中央过滤器可靠地递送控制消息的方法和设备。根据本发明的一个方面，针对客户网络处的检测器与服务提供者的网络处的中央过滤器之间的通信提供通告废除协议。在一个示例性实现方式中，通告废除协议包括一对通信信道。第一通信信道是可靠的、安全认证后的流，如TLS信道。第二通信信道可以是在例如UDP顶部的、不可靠的、认证后的非流协议，其使用安全信道来引导认证。例如，可以采用用户数据报协议（UDP）来避免采用基于TCP的协议的传统技术所需的即时肯定应答。在这种方式下，如果例如由于恶意攻击而使在从中央过滤器到检测器的返回路径中存在大量分组丢失，其中中央过滤器的肯定应答很可能丢失，则仍可以实现所期望的保护。此外，使用在从检测器到中央过滤器的正向路径上对控制消息的冗余发送来克服正向路径上的适中的分组丢失。通常，在攻击期间，优选的是从检测器向中央过滤器发送多个冗余分组，而不是从中央过滤器向检测器发送任意分组。

图1示出了本发明可操作的网络环境100。如图1所示，企业网150使用以下结合图3进一步讨论的检测器300来保护自身免于恶意攻击。企业网150允许企业用户通过服务提供者网络120访问互联网或另一网络。服务提供者网络120向企业网150的用户提供服务，并通过入口端口115接收来自各个源的分组，以及将接收到的分组发送到企业网150中所指示的目的地。

在一个示例性实施例中，检测器300与以下结合图2进一步讨论的中央过滤器200协作，以保护自身免于恶意攻击。通常，如以下进一步讨论的，检测器300将检测对企业网150的恶意攻击（如拒绝服务攻击），并将通知由服务提供者维护的中央过滤器200。

中央过滤器200用于通过服务提供者网络120来限制到达企业网150的业务量。检测器300通常位于企业网150中的防火墙之后，而且检测器300通常向ISP的中央过滤器200发送通告废除消息。基于名称为“Method and Apparatus for Defending Against Denial of Service Attacks

in IP Networks by Target Victim Self-Identification and Control”的美国专利申请11/197,842以及名称为“Method and Apparatus for Defending Against Denial of Service Attacks in IP Networks Based on Specified Source/Destination IP Address Pairs”的美国专利申请11/197,841，可以实现检测器300和中央过滤器200，此处对这两个专利申请进行修改以提供本发明的特征和功能。

在确定了拒绝服务攻击正在进犯企业网150时，检测器300将一个或多个源/目的地IP地址对发送到中央过滤器200，中央过滤器200使服务提供者网络120限制（例如，阻止或速率限制）源IP地址和目的地IP地址与任意所发送的源/目的地IP地址的源IP地址和目的地IP地址相匹配的那些IP分组的发送，从而限制（或消除）一个或多个源设备110对企业网150内的攻击受害者的拒绝服务攻击。可选地，检测器300使用不可靠的UDP连接135或主安全认证连接130来发送源/目的地IP地址对。根据本发明的一个方面，针对检测器300与中央过滤器200之间的通信提供通告废除协议。

因而，拒绝服务攻击的受害者可以通过向服务提供者通告废除攻击者来进行“后推（push back）”，作为响应，该服务提供者将更新要被阻止的源/目的地IP地址对的表。更具体地，在认识到发生攻击时，受害者（企业网150）将识别被认为是攻击的一部分的分组中所指定的一对或多对源/目的地IP地址，并将这些IP地址对传达给服务提供者以由中央过滤器200进行阻止。

如图1所示，将指定了订户（企业网150）的分组分成通常与“好”和“差”业务量相对应的类。例如，分别递送（允许）来自类别A 105-A的好业务量并速率限制或丢弃来自类别B 105-B和类别N 105-N的差业务量。将源计算设备110分到N个示例性分类中的一个中，其中，源计算设备110将业务量发送到与企业网150相关联的目的地地址。通告废除对好业务量与差业务量之间的边界进行移位。

注意，根据特定的示意性实施例，无需将攻击者（即，识别出的一个或多个源IP地址）从网络完全切断，而只是禁止该攻击者向受害者（即，识别出的一个或多个目的地IP地址）发送分组。特别是在识

别出的一个或多个源IP地址表示针对对受害者的给定攻击已被接管的合法用户（例如，僵尸）及相关机器的情况下，这是有利的。因此，被接管的机器的拥有者可以继续出于合法目的使用该系统，然而同时，有利地挫败了正在向受害者（很可能不为合法用户所知）进犯的攻击。此外要注意，根据这些示意性实施例的技术还有利地提供了保护以避免给定的受害者过分热心地识别攻击者。根据本发明的原理，由于对攻击的识别由明显受害者的判断进行处理，因此，明显有利地，只有去往给定受害者的业务量被切断或被限制。

受害者可以通过具有变化的简单或复杂程度的一个或多个算法来辨别恶意攻击，该一个或多个算法在本发明的范围之外，但是对于本领域技术人员而言，其中多个算法是明显的。例如，根据本发明的一个示意性实施例，可以检查分组踪迹，并且可以仅基于来自单个识别出的源或多个识别出的源的非常高的业务量水平（例如，高分组速率）的存在来识别攻击。要注意，这是一种识别拒绝服务攻击的存在的传统方法，并将为本领域普通技术人员所熟知。

然而，在其他实现方式中，可以执行基于应用的、对分组内容和应用日志的分析，以识别具有可疑性质的分组、分组序列或动作，例如：辨别已有对不存在的数据库元素的频繁数据库搜索；辨别已有明显由人发出的多个请求，其发生的速率高于人能发起它们的速率；识别句法上无效的请求；以及识别正常发生的活动的操作中特别敏感时刻的可疑业务量量。例如，如果股票交易网站注意到在即将到来的股票交易期间的敏感时刻的特别具有破坏性的业务量，则可能识别较后一类可疑分组的示例。在此外的变体中，有利地，可以在更复杂的分析中组合可能的攻击的多个不同标记（例如，其可包括一个或多个的上述情况），以识别攻击的存在。

示例性检测系统可以工作于两种模式中的一种。当区域处于“缺省丢弃”模式时，缺省的行为是对除了在缺省丢弃中明确列出的业务量以外的所有指定该区域的业务量进行过滤。通常，在缺省丢弃模式下，除了被明确授权（例如，与预定义的允许过滤器相匹配）的情况以外，过滤器都将自动丢弃所有业务量。另一方面，当区域处于缺省

允许模式时，除了与预定义的丢弃过滤器明确匹配的业务量以外，过滤器使所有去往该订户的业务量通过。

图2是图1中可实现本发明的过程的中央过滤器系统200的示意框图。如图2所示，存储器230配置处理器220以实现此处所公开的拒绝服务过滤方法、步骤和功能。存储器230可以是分布式的或本地的，并且处理器220可以是分布式的或单一的。可以将存储器230实现为电存储器、磁存储器、光存储器或者这些或其他类型的存储设备的任意组合。应当注意，构成处理器220的每一个分布式处理器通常包含其自身的可寻址存储空间。还应当注意，可以将计算机系统200的一些或全部并入专用或通用的集成电路中。

如图2所示，示例性存储器230包括以下结合图4进一步讨论的拒绝服务过滤器规则库260和一个或多个拒绝服务过滤过程400。通常，示例性拒绝服务过滤器规则库260是包含与应由中央过滤器200所限制或允许的业务量相关联的源/目的地地址对的传统过滤器库。拒绝服务过滤过程400是根据本发明的、用于防御拒绝服务或其他攻击的示例性方法。

可以将中央过滤器200实现为服务提供者网络120中包括的单机盒，或备选地，实现为被并入已存在于网络120中的其他传统网元中的线卡（line card）。此外，根据特定的示意性实施例，有利地，网络120内相对靠近攻击原点的位置处的承载者布置中央过滤器200，或者可以首先放置中央过滤器200以有利地使最优客户防御攻击。

图3是图1所示的、可实现本发明的过程的检测器300的示意框图。如图3所示，存储器330配置处理器320以实现此处所公开的拒绝服务过滤方法、步骤和功能。存储器330可以是分布式的或本地的，并且处理器320可以是分布式的或单一的。可以将存储器330实现为电存储器、磁存储器、光存储器或者这些或其他类型的存储设备的任意组合。应当注意，构成处理器320的每一个分布式处理器通常包含其自身的可寻址存储空间。还应当注意，可以将计算机系统300的一些或全部并入专用或通用的集成电路中。如图3所示，示例性的存储器330包括以下结合图5进一步讨论的一个或多个拒绝服务检测过程500。

图4是描述了并入本发明特征的拒绝服务过滤过程400的示例性实现方式的流程图。要注意，针对“缺省允许”模式实现示例性的拒绝服务过滤过程400。对于本领域普通技术人员而言，针对“缺省丢弃”模式的实现方式将会是显而易见的。通常，拒绝服务过滤过程400是根据本发明的、用于防御拒绝服务或其他攻击的示例性方法。示意性的拒绝服务过滤过程400在中央过滤器200处执行并在步骤410期间开始，从检测器300接收拒绝服务攻击正在进犯企业网150中的给定目标受害者的UDP指示。

此后，在步骤420期间，网络承载者从检测器300接收表示为了挫败拒绝服务攻击而应被阻止的IP分组的一个或多个源/目的地IP地址对。示意性地，源IP地址是发起攻击的（例如，“僵尸”）计算设备110的IP地址，而目的地IP地址是与目标受害者自身相关联的IP地址。如以下讨论的，根据DP来发送来自检测器300的消息。

然后，在步骤430期间，网络承载者监控IP分组业务量，以识别源和目的地IP地址与接收到的源/目的地IP地址对中的一个相匹配的那些IP分组。在步骤440期间执行测试，以确定是否一个或多个分组与拒绝服务过滤器规则库260中的地址对相匹配。

如果在步骤440期间确定了一个或多个分组与拒绝服务过滤器规则库260中的地址对相匹配，则在步骤460期间丢弃或限制分组。如果在步骤440期间确定了一个或多个分组与拒绝服务过滤器规则库260中的地址对不匹配，则在步骤470期间允许向企业网150发送该分组。

图5是描述了并入本发明特征的拒绝服务检测过程500的示例性实现方式的流程图。通常，拒绝服务检测过程500是根据本发明的、用于防御拒绝服务或其他攻击的示例性方法。示意性的拒绝服务检测过程500在目标受害者处由检测器300执行并在步骤510期间开始，基于对接收到的IP分组的分析来确定拒绝服务攻击或另一恶意攻击正在进犯该目标受害者。然后，在步骤520期间，识别表示为了挫败拒绝服务攻击而应被阻止的IP分组的一个或多个源/目的地IP地址对。（示意性地，源IP地址是发起攻击的“僵尸”机器110的IP地址，而目的地IP地址是与目标受害者自身相关联的IP地址。）最后，在步骤530期间，使

用所公开的DP将所识别出的源/目的地IP地址对发送到受害者的承载者网络的中央过滤器200，以使承载者网络能够阻止具有匹配的源和目的地IP地址的IP分组的发送。

通告废除协议

在一个示例性实现方式中，检测器300与中央过滤器200之间的通告废除协议（DP）通信信道由针对通告废除的UDP端口和针对大多数其他通信的TLS连接组成。DP事务有两种类型。第一种基于UDP，由从检测器300到中央过滤器200的、可能由来自中央过滤器200的可选响应进行应答的请求分组组成。第二种通常基于TLSv1，由最终在对应的记录中应答的SSL“记录”组成。多数DP事务由检测器300发起。根据本发明的一个方面，多数DP请求不要求响应或肯定应答。

基本的DP事务是从检测器300到中央过滤器200的通告废除。每一个检测器300代表“区域”来说出（speak）作为订户（企业网150）所拥有的IP地址的子集的IP地址集。检测器300被说成“属于”该区域。检测器300通告废除指定其所属区域的业务量。（检测器300自身的IP地址不必是其所属区域的一部分）。

检测器300发起所有的通告废除事务。在订户最不可能想要接收分组时（当其超载时），最有可能发送来自该订户的通告废除。同样在那时，虽然还可能（甚至很可能）从订户到中央过滤器200的路径上的分组丢失率比平常高，并且中央过滤器200可能比平常忙一些，但来自订户的入站（inbound）路径不太可能像遭受攻击的、去往订户的路径一样严重超载。从订户到中央过滤器200的路径处于服务提供者的网络之内。因此，所公开的DP尝试避免在通告废除时向订户发起任何业务量。因此，并没有可靠地发送通告废除——没有从中央过滤器200接收到肯定应答。

更确切地，订户优选地发送每一个通告废除请求的多个副本，而不会让中央过滤器200发送甚至一个响应。该多个副本增大了通告废除请求安全到达中央过滤器200的可能性。例如，如果发送5个副本，并随机丢弃分组，那么即使分组丢失率是20%（且丢弃率通常肯定在5%以下），该请求的至少一个副本将会到达的几率也极高。利用这些示例

性的数字（20%的分组丢失率和5个副本），在假定展开分组发送以使得所有的丢失都独立的情况下，至少一个副本到达的几率仍大于99.96%。

相同的推理还保证使每一个分组都是自持的，以便不会不必要地依赖于按次序到达的分组。如前所示，DP事务一般由企业（通过检测器300）发起，而从不由中央过滤器200发起。这一点部分地是由上述考虑促成的，并且也是为了维护请求/响应模型以对企业周围的防火墙更加友好，并增大DP分组能够安全到达的可能性。

中央过滤器200确定正式安装了哪些过滤器规则。检测器300仅向中央过滤器200发布通告废除。并没有坚定地保证该通告废除将到达中央过滤器200。此外，针对目的地的给定区域，多于一个检测器300可以通告废除不友好的源。因此，检测器300无法确定地知道已安装的过滤器的集合。所期望的是，订户知道实际安装了哪些过滤器、哪些过滤器从未到达中央过滤器200、以及其他检测器300（或由于冲突（如下所示））已移除或创建哪些过滤器。为此，当事情稍微平息下来时，订户可以请求来自中央过滤器200的状态报告。该状态报告列出哪些请求已达到、安装了哪些过滤器以及其他信息（以下详细说明）。

为了可靠地接收该状态并引导认证，所公开的DP提供了每一个检测器300与中央过滤器200之间的（可靠）通信信道（TLS）。

中央过滤器200和每一个检测器300必须协作以维护一些共享状态。最明显的共享状态是已安装的过滤器规则的集合，但还存在与DP自身相关的其他共享状态，如通告废除的序列号和用于认证的信息。该示例性实施例只要求适度同步的时钟。为了避免对在检测器300或中央过滤器200上运行不必要的任何东西的需要，所公开的DP提供了非常粗时钟“同步”，从而不需要运行以下在名为“B 认证”的部分中所讨论的网络时间协议（NTP）。无论如何，很多订户将希望在检测器300上运行NTP，以简化企业网上的事件相关性（但这不是DP工作所需要的）。

对于过滤器和协议状态，所公开的DP命令检测器300和中央过滤器200就初始共享状态可靠地达成一致，然后，两侧都留意该状态随时

间的改变。在检测器300与中央过滤器200之间不相符的情况下，中央过滤器200总是具有共享状态的“真实”描绘。保持同步的过滤器状态的量取决于检测器300（其可能根本不考虑过去的通告废除，并使其所有的分析都基于当前的业务量流）。DP需要协议状态。

检测器300可以通过周期性的状态请求来与中央过滤器200重新同步过滤器状态。通常，中央过滤器200只返回自上一个状态请求起的过滤器状态改变（虽然也可以返回所有当前活动的过滤器而不管是何时安装的，如果被这样请求了的话）。通常，中央过滤器200返回该区域中所有检测器300的过滤器，但如果被请求，则可以只返回由该检测器300请求的通告废除。

检测器300可以通过同步请求来重新同步序列号和认证密钥。在同步事务中，检测器300单方面地选择新的序列号，并且中央过滤器200产生用于认证的新会话密钥。

在检测器300崩溃或不知何故丢失信息的情况下，检测器300可以请求所有过滤器规则而不仅仅是最近的过滤器规则。在任何时候，检测器300都可以重新协商用于通告废除的认证信息（如下所示）。

在中央过滤器200重新设置所有过滤器规则（区域改变、模式改变或一些致命的数据库崩溃）的情况下，中央过滤器200故意忘记其与检测器300的关联，提示下一检测器事务返回来自中央过滤器200的重新同步响应。当检测器300与中央过滤器200进行重新同步时，中央过滤器200可以告知检测器300其先前的状态不再有效；这需要请求完整的状态。

中央过滤器200可以接收残缺的（malformed）或未经认证的分组。在这种情况下，中央过滤器200向（合法的）发送者返回错误分组，例如，对于每一个主机最多到每30秒一个错误分组的最大速率。例如，可以设置速率限制以避免攻击者使用通告废除协议来发动拒绝服务攻击。

冲突通告废除

如果分组与分类相匹配，则通告废除可以指定多个不同的可能动作。因而可能会发生冲突。例如，一个检测器300可以指出，整个子网

似乎将发动网络爬虫（web crawler）并应被限制速率。另一检测器300可以检测发动实际攻击的该子集中的特定主机，并指出应当丢弃来自该主机的所有分组。在这种有冲突的情况下，毋庸置疑，与前一个规则相比，后一个规则更为明确：其涉及单个主机，并表示要丢弃而不是仅对该源进行速率限制。在这种冲突中，有理由主张更严格的规则适用。然而，假设所请求的动作是相反的：一个检测器300请求对单个源进行速率限制，而另一检测器300请求丢弃来自该子网（包括该源）的所有分组。可以主张前一个规则更明确（其涉及单个主机而不是整个子网）或完全平等地主张后一个规则更严格（其表示要丢弃分组而不是仅将其变少）。该示例性实施例采用了最明确的源地址优先的惯例。

然而，为清楚起见，对于检测器300而言最佳的实践是避免发布冲突规则。在发布新的集合之前总是可能取消现有的冲突规则。然而，假定通告废除不可靠，可以想到，在发现更早的冲突规则被取消之前，中央过滤器200将接收新的规则。此外，假定多个检测器300管理相同的区域，两个检测器300可能独立地发布冲突通告废除而没有放弃冲突。

应当指定中央过滤器200在遭遇冲突时的行为。在一个示例性的实现方式中，基本策略是：在有冲突的情况下（两个规则具有相同的源地址指定，但具有两个不同的动作和原因），较晚的规则推翻较早的规则。（“较后的”指的是在规则到达中央时）

DP协议算法

A. 可靠的发送

如上所讨论的，应当将分组从检测器300发送到中央过滤器200，而不是沿另一个方向从中央过滤器200发送到检测器300。此外，每一个分组可以自我支持而不需要按次序递送。因此，所公开的DP通过发送每一个分组的多个副本来选择在概率上改进成功到达的几率，而不是保证每一个通告废除分组都到达，并依次到达。例如，响应于同步（SYNCH）请求，在UDP分组中将DP通告废除请求发送到所指定的中央过滤器200上的端口。通常，将每一个通告废除分组发送P次，而

且不需要肯定应答。在一个示例性的实现方式中，P被固定为5，并且不提供对分组步长的正式要求。

针对次序的要求（假定规则为：在冲突消解规则没有选择清楚赢家的直接冲突过滤器规则的情况下，最新的规则推翻较早的规则），根据应用来传递DP序列号以确定发送次序。针对来自多个检测器300的通告废除，中央过滤器200充当串行化器。通过序列号对来自单个检测器300的请求明确地进行排序。中央过滤器200单方面地决定交织的次序。中央过滤器200记住每一个检测器300按照全局次序在何处最后接收到状态响应。

发送多个分组背后的意图是确保每一个分组的至少一个副本到达中央过滤器200，而不是用分组来泛滥中央过滤器200。此外，攻击者不应具有借以对所公开的DP发动DoS攻击的施加点（point of leverage）。平均下来，中央过滤器200应对每个事务处理一个分组。中央过滤器200认证每一个分组以确定其被正确的检测器300所发送的要求意味着分组处理可能成本较高。

在无需高成本的计算的情况下可以丢弃大多数冗余分组。在一个实现方式中，首先执行成本最低的测试。例如，序列号未被加密，且该序列号检查通告废除请求在计算上成本较低。类似地，检查检测器名称是否是已知的成本也较低。在执行其他测试之前，易于丢弃复制的请求和超出范围的序列号。

在所公开的DP中，检测器300基于UDP发起通告废除事务。针对其他请求，DP维护了单独的TLS连接（基于TCP）。

B. 认证

在该示例性实现方式中DP的基本认证机制是由具有客户端证书的TLSv1提供的认证握手。将受托的ISP证书权力机构的公共密钥预先加载进中央过滤器200和每一个检测器300中。每一个检测器300和中央过滤器200具有针对由该认证权力机构（CA）签名的公共密钥的证书。此外，向订户检测器300提供中央过滤器200的完全合格的域名，该域名也是服务器证书主题的CN部分。

密钥与检测器的“名称”相关联，而不是与检测器的IP地址相关联，其IP地址可能由于多种原因而改变。如下所提到的，在任何时候，DP强制具有给定名称的一个检测器300的最大值。遵循标准的TLS协议，中央过滤器200发送证书请求消息，该消息指定了中央过滤器200将只接收由CA签名的证书。作为客户端认证过程的一部分，检测器300使用两个消息作出响应。首先，检测器300提供包含检测器的名称和检测器的公共密钥的证书。其次，检测器300发送证书校验消息，该消息包含由检测器的私有密钥签名的所有TLS握手消息的摘要。现在，中央过滤器200可以将客户端认证为在证书中所提到的检测器300。

一旦建立了TLSv1连接，在可以基于UDP发布任何通告废除之前，中央过滤器200就应使用安全加密信道向检测器300发送随机选择的160比特的秘密随机数（nonce）。

认证每一个DP通告废除分组。在一个示例性实施例中，所公开的DP中的通告废除是由以下（a）、（b）、（c）和（d）的加密散列（hash）认证的：（a）UDP分组内容；（b）计时器（自RSTART起的“单位”数，其中在同步期间建立了“单位”的长度和RSTART的时间）；（c）秘密随机数；以及（d）TLS信道所使用的DP端口号。（b）是对重放攻击的最小防御，（c）向中央过滤器200认证检测器300。该示例性实施例中所使用的MAC功能是HMAC-SHA1（详情参见互联网RFC 2104），上述额外字段被用作HMAC密钥。

分组中可以包括20比特的序列号，并且假定在单位计数器递增之前，每一个服务器发送少于2^{20}个请求。DP的端点只接受具有给定序列号的第一有效分组。到序列号绕回时，单位计数器已递增以防御简单的重放攻击。检测器300包括作为序列号高位比特（第21个比特）的单位计数器号码的低位比特。这就允许“日期”（自RSTART时间起的单位数）在检测器300上以相对于中央过滤器200的任意时间改变，并且中央过滤器200仍可以计算出隐藏日期是什么（只要每“天”（单位）有至少一个同步交换）。这就允许避免了对紧同步时钟的需要。

在检测器300试图在时间单位内发送多于2^{20}个分组的不太可能的情况下，检测器300应当请求来自中央过滤器200的新的安全随机数。

检测器300对单位的长度（表示为一天的几分之几）进行选择以使序列号不太可能绕回。

计算这些加密散列可能看起来成本较高，并且发送每个分组的多个副本可能会使费用剧增。然而，需要注意，一旦成功接收到给定的序列号，在无需计算散列的情况下便可以丢弃任何副本。来自攻击者的随机构建的分组不太可能被接受，这是因为可接受序列号的窗口与整个序列号空间相比非常小。中央过滤器200丢弃所期望的窗口之外的分组。此外的开窗可以基于检测器的名称：例如，可以在2字节的字段内以大约100个有效值稀疏地分配检测器的名称。

如果考虑到攻击者可能窥探（snoop）到通告废除请求，同时复制检测器的名称、捕获序列号、然后发送窗口中最后一个分组的多个差的副本，则可以提供一种抵御窥探器的快速丢弃方法。实际上，期望将不必须有这种额外水平的保护——在接收机处，执行SHA1散列的成本将不是证明所增加的复杂度的合理性的充分瓶颈。然而，以下讨论该安全快速丢弃方法。

C. 安全快速丢弃

安全快速丢弃方法是可选的。在示例性的DP版本中的通告废除分组中提供了针对该可选方法的空间，但除非实际确定了需要该保护，不然将不会在DP中启用该安全快速丢弃算法。

基本途径如下：每一个通告废除请求将包括：计算L比特字符串S_L的简易性（临时地，L=5，以使得该字符串适合于序列号字段的填充）。S_L是序列号与由中央过滤器200在SSL信道上提供的秘密密钥对的简单函数的结果。在计算上，检验分组是否有效的成本不高——如果S_L不是所期望的值，则丢弃分组。确定分组是否有效仍然需要对加密散列的检验——但大约每序列号发生一次。

当检测器300与中央过滤器200对HMAC-SHA1散列的共享密钥进行同步时，中央过滤器200还应提供字符串长度L、密钥长度B、B+L比特的字符串S、以及小整数K，以使得$1 \leq K \leq B$。这些都不为攻击者所知，虽然L和B可能改变不频繁且在与S和K相同的意义上不应被视为“秘密”。针对具有序列号s的通告废除请求，S_L是在比特位置b处开

始的S中的L比特子串。b是s、B和K的函数。将S_L插入分组的HMAC-SHA1散列的第b0个位置处（将SHA1散列的长度扩展L个比特）。

如果L=5且B=1019，那么直到大约2^{20}个通告废除分组时图案才会重复——此时，在任何情况下都必须针对HMAC-SHA1散列选择新的随机数。假定在窥探的攻击者看来，字符串S_L是随机的，对S_L的简单检验应以因子2L使得攻击分组的流变少。然而，选择更大的L增加了攻击者可重构S然后重构K的几率，因此L应被选择以使得$2L2^L<B$（意味着L是O(logB)）来避免这种问题（以便每个可能的L比特子串很可能在S中出现多于一次）。

D．DP消息服务

所公开的DP提供了用于检测器300和中央过滤器200的手段以彼此可靠地发送消息。SSL/TLS实现了流中的记录。可以将SSL记录用作DP记录，每一个记录以简单描述了该记录的类型（如状态（STATUS）、消息和状态应答）的DP记录报头开始。然而，经验中，并不是所有的TLS实现方式都在其向客户端的API中保存记录边界（SSL写（除非数据太大）产生SSL记录，而SSL读可以返回部分记录或多个记录）。因此，为了提供跨平台的最大便携性，DP的示例性实施例（可能冗余地）在SSL记录内实现其自身的记录标记协议。理想地，一个DP记录应在每一个SSL记录内都适合——不论如何，记录协议都将生效。DP使用记录起始标记来开始该记录，并使用记录结束标记来结束记录。每一个记录以类型和长度字段开始。长度字段允许避免比特/字节填充——起始记录标记或结束记录标记出现在该记录内是正当的。长度字段是消息内不包括报头和报尾的字节的数目。

虽然在该示例性实施例中起始标记和结束标记是4字节序列，但没有对DP消息的对准要求。消息的主体可以是任意长度，该长度不必是32比特（4个字节）的倍数。在服务器或客户端发布残缺的记录的情况下，起始标记和结束标记允许恢复记录边界——只需要搜索序列[记录结束][记录起始]，其后紧跟有自身指向[记录结束][记录起始]对的长度字段。

E．分组格式、版本号和兼容性

对所公开的DP的修改应当是后向兼容的。对利用SSL信道的协议操作的不兼容修改将会分配新的记录类型标识符，而不是重新使用具有不兼容格式的旧类型。对通告废除事务的不兼容改变将会要求选取新的DP端口号作为所修改的DP规范的一部分。DP将采用两种方式之一在DP信道的远端处检测非DP代理。SSL连接的远端将无法认证或将无法遵循DP初始同步协议。如果在SSL连接建立期间由于某些原因没有检测到不兼容性，则密码散列将不能用于UDP业务量，这是因为该远端不是DP或在散列中正在使用对于DP不兼容的版本号。这就避免了对DP有线发送的数据中的版本号或幻数的需要。

分组和操作

如前所示，检测器300在DP信道上与中央过滤器200进行通信。当前应当建立DP信道以便检测器300与中央过滤器200进行通信。每一个检测器300都与中央过滤器200的一个具体示例绑定。中央过滤器200将不会与不与其绑定的检测器300进行通信。与给定中央过滤器200绑定的每一个检测器300具有由该中央过滤器200使用的数字“名称”。

建立DP信道的第一步是发起从检测器300到中央过滤器200的SSL/TLS连接。通过SSL/TLS认证过程，中央过滤器200将进行通信的检测器300识别为可信的。在TLS握手的客户端认证阶段，检测器300要求成为在检测器300向中央过滤器200所提供的证书中所使用的名称。该名称应当具有预定义的形式。

一旦建立了TLS信道，检测器300就必须在TLS信道上发送同步请求。直到从检测器300向中央过滤器200发送了同步请求并且从检测器300向中央过滤器200返回了同步肯定应答时，TLS信道才被视为已被初始化。除其他值以外，示例性同步请求还包括下一个通告废除事务的序列号（每一个通告废除事务的序列号将加1，直到下一个同步请求为止）。还初始化“时间单位”的长度以及随机开始时间“RSTART”。中央过滤器200响应同步肯定应答，该同步肯定应答包括：随机产生的160比特会话密钥、和检测器300是否可以满足增量过滤器状态或是否需要完全过滤器状态的指示。

在该交换后，检测器300必须建立路径MTU，并请求和接收第一状态答复。在这一点上，建立DP信道。如上所述，DP事务有四种基本类型：同步、通告废除、状态查询、和消息。前三种事务类型（同步、通告废除、和状态查询）都由检测器300发起。然而，响应于检测器300或中央过滤器200的请求，可以在SSL信道上沿两方向中的任一方向发送消息。

在UDP信道上将通告废除事务从检测器300上的随机端口发送到中央过滤器200上的DP端口。在正常情况下，中央过滤器200根本不发送响应。在错误、失败或潜在攻击的情况下，中央过滤器200可以响应重新同步或错误分组。当已知仍然存在TLS信道时，在TLS信道上发送这些响应。当不存在TLS信道时，基于UDP发送响应（在这种情况下，该响应必须是重新同步消息）以重新建立TLS信道。一般的规则是：如果进入的分组是形状完备的，并且中央过滤器200相信客户端是合法的，则中央过滤器200发送重新同步消息。否则，中央过滤器200发送错误消息。

所有其他事务利用TLS信道。

A．UDP事务（通告废除和响应）

如前所示，基于分组的内容以及包括随机数、日期计数器和全局DP端口号的密钥，来计算HMAC-SHA1消息认证。图6示出了针对UDP分组预先考虑的、用于UDP请求的HMAC密钥。

如上所示，自RSTART起的单位数防止DP成为DoS攻击源。

B．SSL信道

在TLS信道上发送的所有DP通信都被分解为记录。在一个示例性实施例中，单个DP记录的最大大小是16000字节。在向SSL协议的API允许之处，每SSL记录刚好有一个DP记录是很好的惯例。示例性的DP记录开始于例如预定义的4字节序列，结束于另一个预定义的4字节序列。将DP记录的类型（以网络字节的次序）编码为直接跟在消息起始标记之后的32比特整数。将DP记录的长度（以网络字节的次序）编码为直接跟在类型之后的32比特整数。图7示出了DP记录报头和报尾在安全可靠流内的示例性布局。

本发明可以结合一个或多个的辅助工具进行工作。例如，这样的工具可能包括用于辨别所施加的拒绝服务攻击的互联网服务器插件程序（plug-in）、向各种IDS系统（侵入检测系统）的链接、用于网络诊断的数据库（如上所讨论的）、以及用于针对在给定的承载者的基础结构内放置清除器（Zapper）功能提供向导的方法。根据此处的公开，提供这些辅助工具中各种辅助工具的本发明的示意性实施例对于本领域技术人员而言是显而易见的。

系统和制造品的细节

如本领域公知的，此处讨论的方法和设备可以被分发为本身包括计算机可读介质的制造品，在该计算机可读介质上实现有计算机可读代码装置。与计算机系统相结合，计算机可读程序代码装置可操作为执行全部或一些步骤，以执行此处讨论的方法或创建此处讨论的设备。计算机可读介质可以是可记录介质（例如，软盘、硬驱动器、压缩盘、存储卡、半导体器件、芯片、专用集成电路（ASIC）），或可以是传送介质（例如，网络，包括：光纤、万维网、电缆、或者使用时分多址、码分多址或其他射频信道的无线信道）。可以使用适合与计算机系统一起使用的、能够存储信息的已知或已开发的任何介质。计算机可读代码装置是允许计算机读取指令和数据（如磁介质上的磁变化或压缩盘表面上的高度变化）的任何机制。

此处所述的计算机系统和服务器均包含存储器，该存储器将配置关联的处理器以实现此处所公开的方法、步骤和功能。存储器可以是分布式的或本地的，并且处理器可以是分布式的或单一的。可以将存储器实现为电存储器、磁存储器、光存储器或者这些或其他类型的存储设备的任何组合。此外，术语“存储器”应当被足够宽泛地解释为包括能够从由关联处理器访问的可寻址空间中的地址读取或能够写入该地址的任何信息。使用该定义，网络上的信息仍处于存储器内，这是因为关联处理器可以从网络取得该信息。

应当理解，此处所示和所述的实施例和变体仅仅用于说明本发明的原理，在不背离本发明的范围和精神的情况下，本领域技术人员可以实现各种修改。

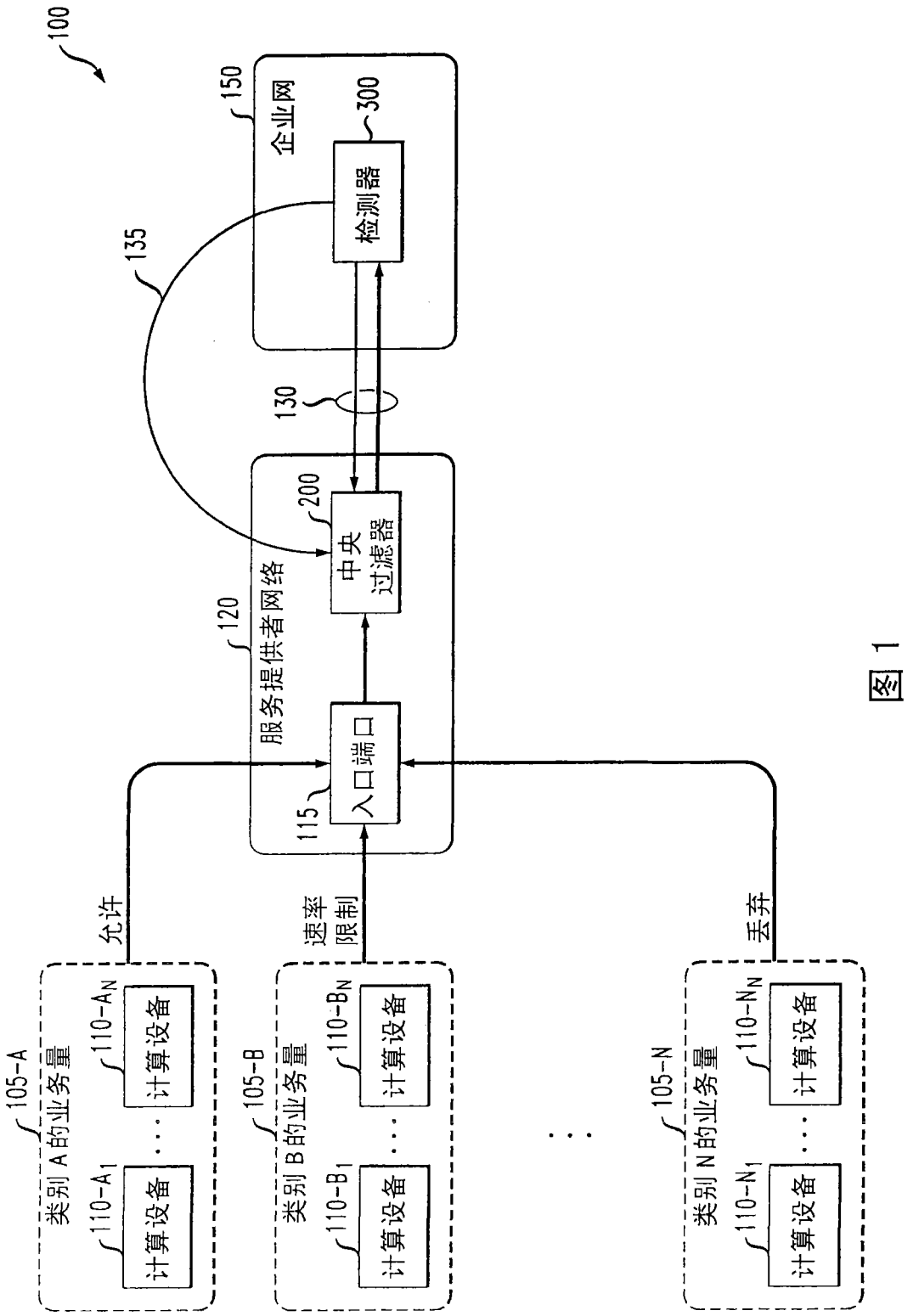

100
150
企业网
检测器
300
135
130
200
中央
过滤器
120
服务提供者网络
入口端口
115
允许
速率
限制
丢弃
105-A
类别 A 的业务量
110-A1
计算设备
110-AN
计算设备
105-B
类别 B 的业务量
110-B1
计算设备
110-BN
计算设备
105-N
类别 N 的业务量
110-N1
计算设备
110-NN
计算设备

图 1

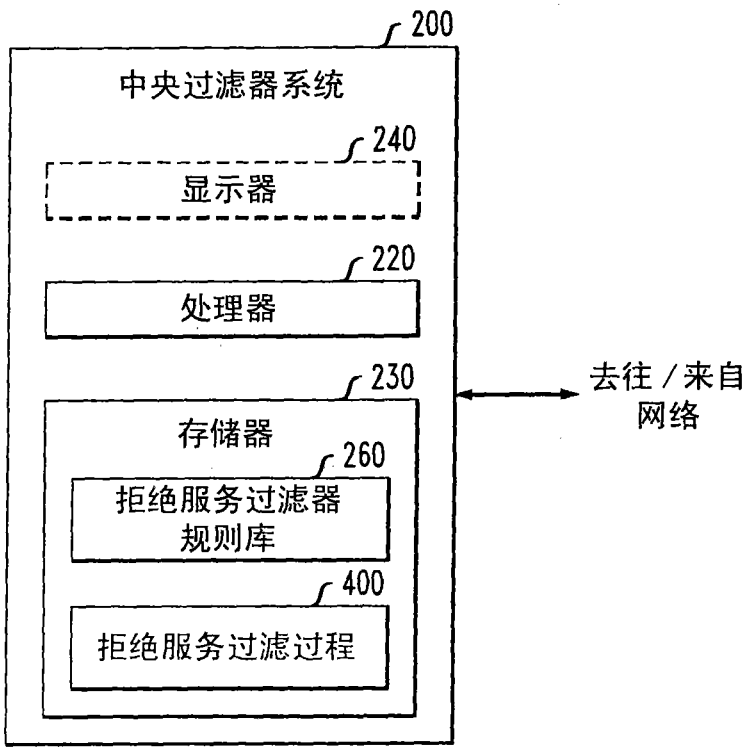

200
中央过滤器系统
240
显示器
220
处理器
230
存储器
260
拒绝服务过滤器
规则库
400
拒绝服务过滤过程
去往/来自
网络

图 2

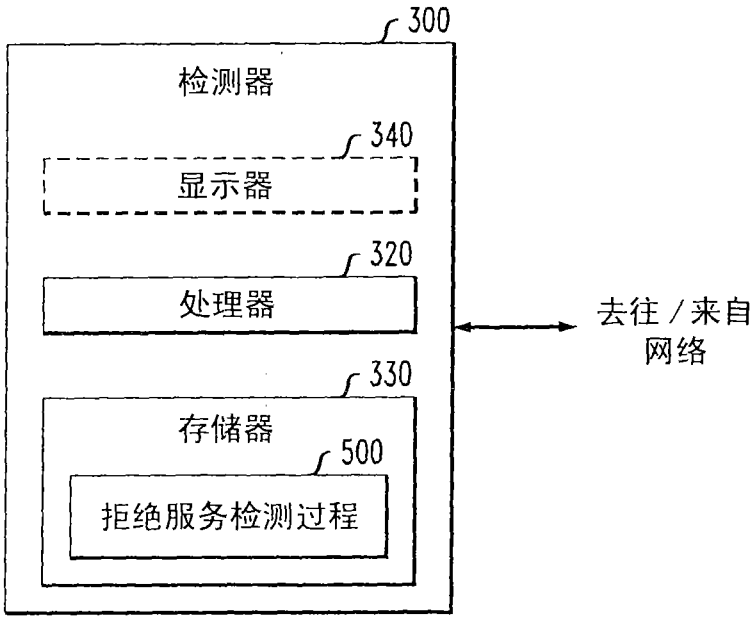

300
检测器
340
显示器
320
处理器
330
存储器
500
拒绝服务检测过程
去往/来自
网络

图 3

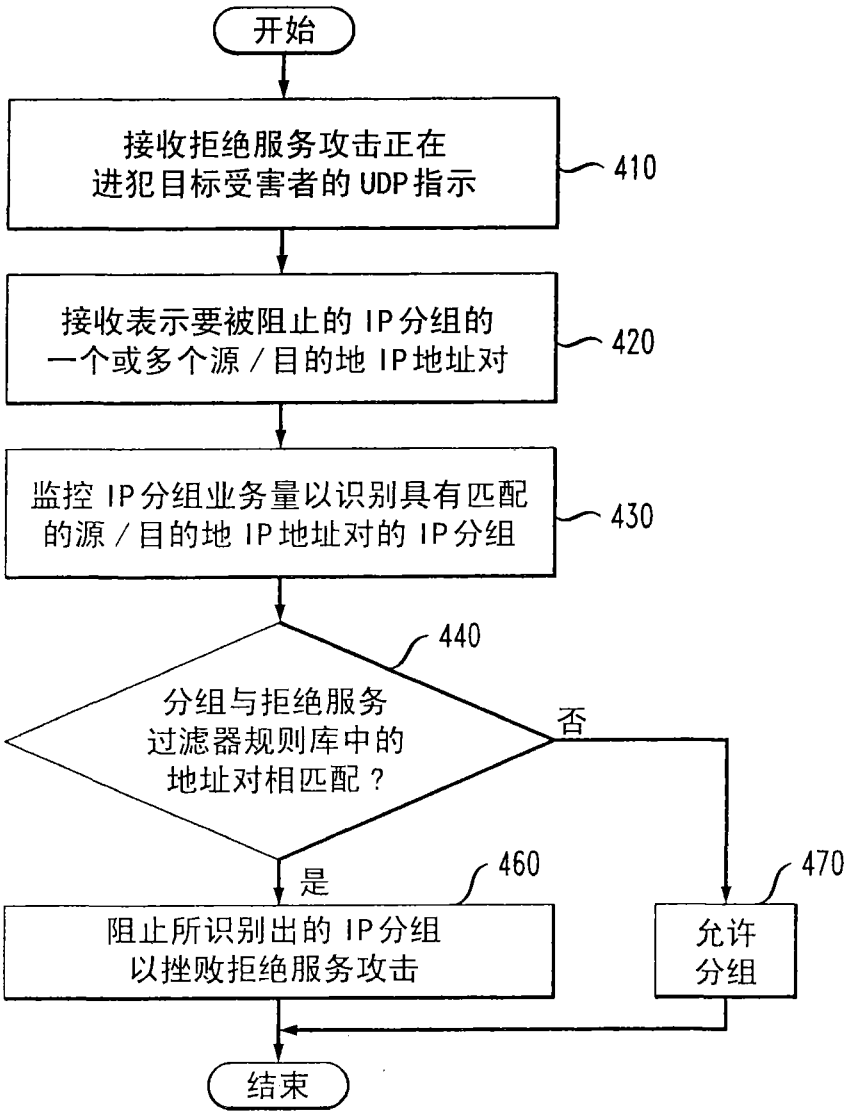

开始
接收拒绝服务攻击正在进犯目标受害者的UDP指示
410
接收表示要被阻止的IP分组的一个或多个源/目的地IP地址对
420
监控IP分组业务量以识别具有匹配的源/目的地IP地址对的IP分组
430
440
分组与拒绝服务过滤器规则库中的地址对相匹配？
否
是
460
阻止所识别出的IP分组以挫败拒绝服务攻击
470
允许分组
结束

图 4

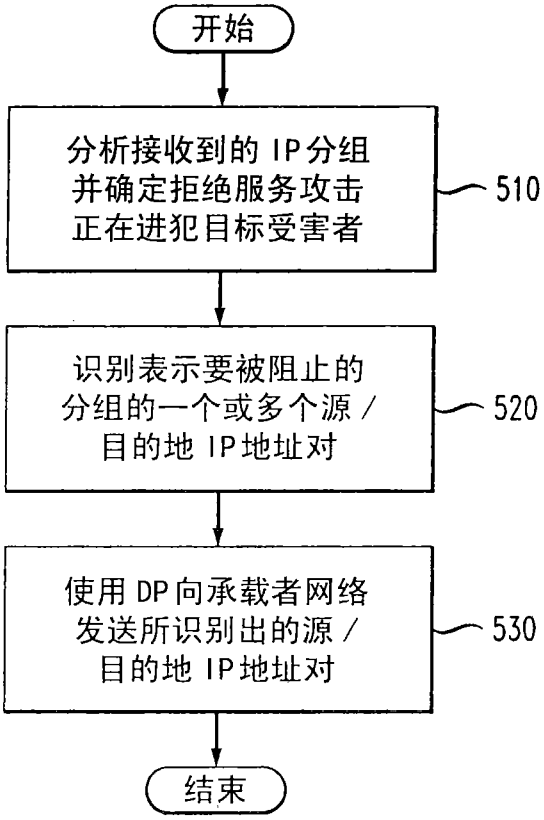

开始
分析接收到的 IP分组
并确定拒绝服务攻击
正在进犯目标受害者
510
识别表示要被阻止的
分组的一个或多个源 /
目的地 IP地址对
520
使用 DP向承载者网络
发送所识别出的源 /
目的地 IP地址对
530
结束

图 5

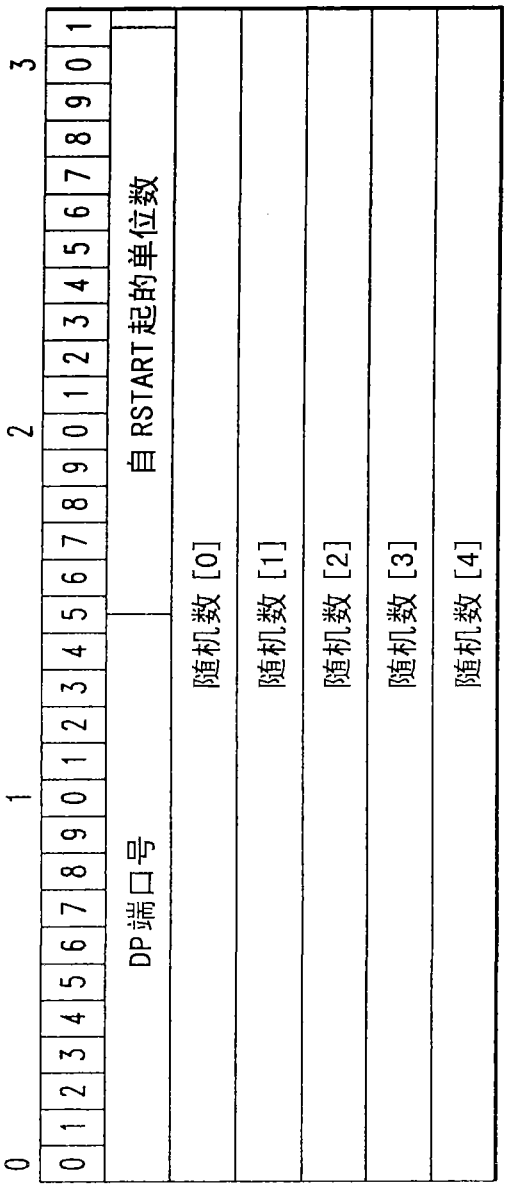

0
1
2
3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
DP端口号
自 RSTART起的单位数
随机数 [0]
随机数 [1]
随机数 [2]
随机数 [3]
随机数 [4]

图 6

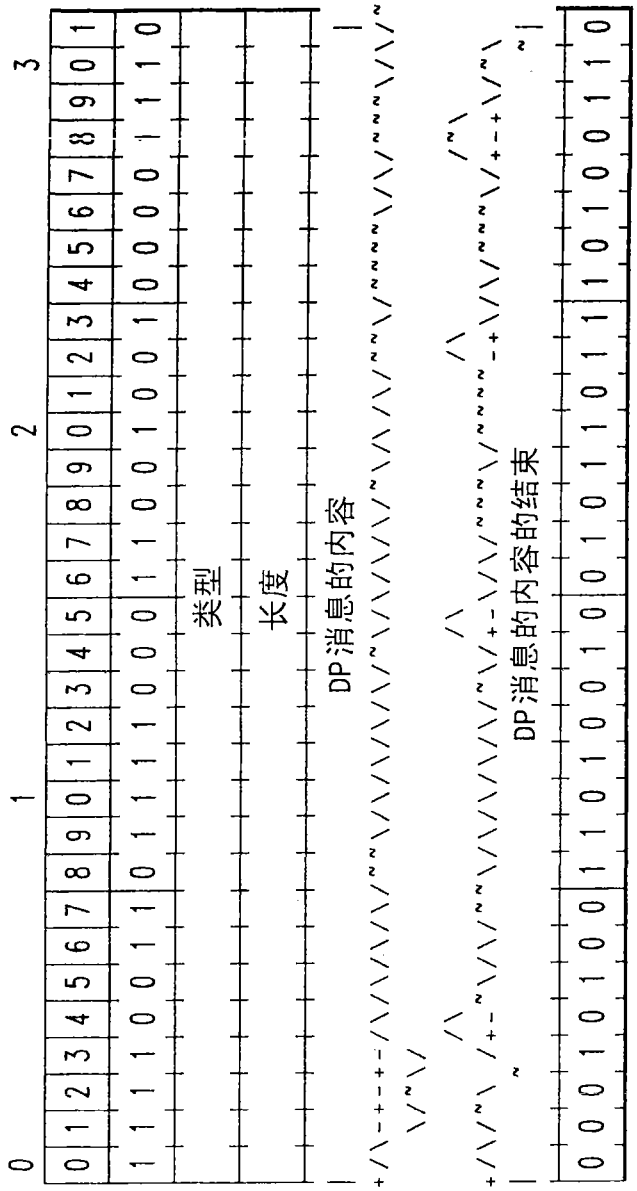

0
1
2
3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
1 1 1 1 0 0 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0
类型
长度
DP消息的内容
DP消息的内容的结束

图 7