[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 12/24 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510079924.6

[43] 公开日 2006 年 3 月 22 日

[11] 公开号 CN 1750536A

[22] 申请日 2005.6.27
[21] 申请号 200510079924.6
[30] 优先权
[32] 2004. 9.14 [33] US [31] 10/940,558
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 C·D·杰弗里斯 R·W·丹福德
T·D·埃斯卡米拉
K·D·希贝格尔

[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 杨晓光

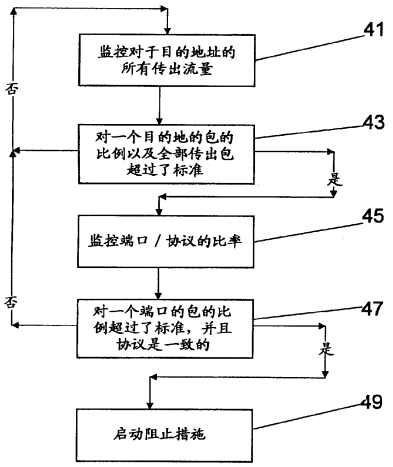
权利要求书 3 页 说明书 14 页 附图 4 页

[54] 发明名称

管理拒绝服务攻击的方法和系统

[57] 摘要

用于在多处理器环境中管理拒绝服务攻击的一种方法、系统和产品。 第一步是建立该多处理器环境中的正常的流量使用基线。 一旦建立了该基线，下一步是监控传出流量以检测被发送至一个特定目标地址的大比例的包，以及与所述基线比较的大量的传出包。 下一步是监控端口和协议以检测发送到一个特定端口的大比例的包，以及发向该端口的所有包对一协议的一致使用。 如果存在这样的发向该端口的所有包对一协议的一致使用以至于证明了拒绝服务攻击，则启动阻止措施以减缓明显的拒绝服务攻击。



1. 一种在多处理器环境中管理拒绝服务攻击的方法，包含如下步骤：

建立该多处理器环境中的正常的流量使用基线；

监控传出流量以检测发送到特定目的地址的大比例的包，以及与所述基线相比的大量的传出包；

随即监控端口和协议以检测发送到特定端口的大比例的包，以及发向该端口的所有包对一协议的一致使用；以及

随即启动阻止措施以减缓明显的拒绝服务攻击。

2. 权利要求 1 的方法，其中所述拒绝服务攻击是传出的拒绝服务攻击。

3. 权利要求 1 的方法，包含如下步骤：

a. 监控对于目的地址的传出流量；

b. 如果（i）对一特定目的地址的包的数量与（ii）传出包的全部数量的比率大于一当前数字，并且传出包的全部数量超过一预置值，则监控选定的端口和协议；

c. 如果（i）对一端口的包的数量与（ii）对所有端口的包的全部数量的比率大于一预置值，并且如果所使用的协议在一大部分端口中是一致的，则开始阻止措施。

4. 权利要求 1 的方法，其中所述多处理器环境是网格计算机环境。

5. 一种包括至少一个网络中的多个计算机的多处理器系统，所述多个计算机适于同时地处理一单个问题，并且还适于由一方法管理拒绝服务攻击，该方法包含如下步骤：

建立该多处理器系统中的正常的流量使用基线；

监控传出流量以检测发送到特定目的地址的大比例的包，以及与所述基线相比的大量的传出包；

随即监控端口和协议以检测发送到特定端口的大比例的包，以及发向该端口的所有包对一协议的一致使用；以及

随即启动阻止措施以减缓明显的拒绝服务攻击。

6. 权利要求5的多处理器系统，其中所述拒绝服务攻击是传出的拒绝服务攻击。

7. 权利要求5的多处理器系统，包含如下步骤：

a. 监控对于目的地址的传出流量；

b. 如果（i）对一特定目的地址的包的数量与（ii）传出包的全部数量的比率大于一当前数字，并且传出包的全部数量超过一预置值，则监控选定的端口和协议；

c. 如果（i）对一端口的包的数量与（ii）对所有端口的包的全部数量的比率大于一预置值，并且如果所使用的协议在一大部分端口中是一致的，则开始阻止措施。

8. 权利要求5的多处理器系统，其中所述多处理器环境是网格计算机环境。

9. 一种包含计算机可读代码的数据存储媒介，所述计算机可读代码适于配置和控制具有至少一个网络中的多个计算机的多处理器环境，所述多个计算机适于同时地处理一单个问题，并且还适于管理拒绝服务攻击，所述的计算机可读代码指引如下步骤：

建立该多处理器环境中的正常的流量使用基线；

监控传出流量以检测发送到特定目的地址的大比例的包，以及与所述基线相比的大量的传出包；

随即监控端口和协议以检测发送到特定端口的大比例的包，以及发向该端口的所有包对一协议的一致使用；以及

随即启动阻止措施以减缓明显的拒绝服务攻击。

10. 权利要求9的数据存储媒介，其中所述拒绝服务攻击是传出的拒绝服务攻击。

11. 权利要求9的数据存储媒介，包含如下步骤：

a. 监控关于目的地址的传出流量;

b. 如果（i）对特定目的地址的包的数量与（ii）传出包的全部数量的比率大于一当前数字，并且传出包的全部数量超过一预置值，则监控选定的端口和协议;

c. 如果（i）对一端口的包的数量与（ii）对所有端口的包的全部数量的比率大于一预置值，并且如果所使用的协议在一大部分端口中是一致的，则开始阻止措施。

12. 权利要求 9 的数据存储媒介，其中所述多处理器环境是网格计算机环境。

管理拒绝服务攻击的方法和系统

技术领域

本发明涉及拒绝服务攻击的检测、识别和减缓。更特别地，本发明涉及这样一种系统、方法和产品，其用于增加系统对系统硬件、软件或数据免受未授权访问的保护的扩展，也用于保护系统免于用作恶意引起的拒绝服务攻击、毁坏数据和软件以及未授权修改的平台。

背景技术

a. 概述

在普遍的商业部署能出现之前，网格计算的设计者必须解决一些挑战。一个这样的挑战是特定网格计算实现的经济生存能力。在很大程度上，一个特定网格计算实现的经济生存能力取决于三个因素：可靠性、安全性和武器装备。这里使用的可靠性指计算等待时间保证。这里使用的安全性指防止对网格上的数据存储器中的数据的危害。这里使用的武器装备指网格避免被用作一个在分布式拒绝服务(DDoS)攻击中可识别的实体的抵抗力，并且特别是避免被恶意接管并转变为一个对其他计算机资产发起 DDoS 攻击的平台的抵抗力。

b. 网格计算

网格的概念一般指这样的一种分布式计算的形式，在该种形式中将遍布于分散的组织和场所中的各种技术组件，如 PC 和存储设备，链接起来以解决一单个大型计算问题。

一个典型的网格 11 如图 1 所示。完全作为说明而不是为了限制，网格 11 包括了一般地显示为工作站的五个元件：111、113、115、117 和 119。

但是，单个元件本身可以是子网格、LAN、WAN 和处理器。图 2 说明了网格 11 及其元件 111、113、115、117 和 119，以及一个通过互联网 223 访问网格 11 的客户端工作站 221。

在此情境中，网格计算是将一个或多个网络中的许多计算机的资源的同时应用于一单个问题—通常是应用于一个需要大量的计算机处理周期或访问大量数据的科学的或技术的问题。在公共领域中的一个著名的网格计算的例子是进行中的 SETI（搜索地外智能）@Home 项目，在该项目中几千人在对来自外层空间的“理性的”信号的迹象的广泛搜索中共享他们的 PC 中不用的处理器周期。

网格计算需要使用能够将一个程序分开并把其各部分转包给多达几千台计算机的软件。网格计算可被认为是分布式的、大规模的群集计算和一种网络分布式并行处理的形式。网格计算可以限于一个企业内的计算机工作站的一单个网络，或者网格计算可以是多个网络的协作，例如一个公众协作（在这种情况下，网格计算有时也被称为对等计算的一种形式）。

网格计算的优势包括：（1）更划算地使用给定数量的计算机资源的能力，（2）解决这样的问题的一种方式，这些问题除此之外没有庞大数量的计算能力就无法解决，（3）这样一个概念，即能够合作地并可能协合地支配和管理许多计算机资源，作为为了一个共同目标的协作。在某些网格计算系统中，计算机可以协作，而不是由一台管理计算机指挥。

网格的种类

网格可以是数据网格或者计算网格。

数据网格是用于共享信息的网格。在高级别的数据网格中，信息共享就像在因特网上访问信息，但具有比传统方式获得的更深的内容，以及在计算资源方面对更“繁重的工作”或努力以及强度的更多需求。

另一方面，计算网格是为了繁重的数字处理，以及为了压缩得出答案必需的时间。IBM 通过 grid.org 支持的天花和炭疽网格就是这样的例子。

安全和隐私

网格控制者必须完全地考虑好安全和隐私的问题，特别当网格将是一个多公司或多实体的项目时。没有建立安全措施的实体冒着被攻击的危险，该攻击来自拥有网格上的一台能够“窃听”在该单元运行的网格计算、并甚至分发用于随后的拒绝服务攻击的僵尸软件的机器的任何人。

c. 拒绝服务攻击

在因特网上，一个拒绝服务攻击（DoS）是这样的一次事件，在此事件中用户或者组织被剥夺了他们通常会期望获得的资源的服务。典型地，服务的丧失是特定网络服务如电子邮件、定单输入、事务处理或数据库管理的无法使用，或者整个网络连通性和服务的暂时性丧失。在最坏的情况下，例如，一个被数百万人访问的网站，如在线银行、信用卡处理、航线和其他旅行预订处理、电子商务、和在线拍卖服务，有时会被迫暂时停止运行。拒绝服务攻击也能够毁坏计算机系统里的程序和文件。尽管拒绝服务攻击通常是故意的和恶意的，不过它有时会意外地发生。拒绝服务攻击是对于一个计算机系统的这样的一类安全违背，其通常不会导致信息的被窃或者其他安全性的损失。不过，这些攻击会耗费目标个人或实体大量的时间和金钱。

图 3 说明了网格 11（及其一般地表示为工作站的元件: 111、113、115、117 和 119）以及通过互联网 223 访问网格 11 以启动一个 DDoS 攻击 341 的客户工作站 221，该 DDoS 攻击 341 是通过在网格元件 115 和 117（被接管而成为僵尸）中植入有害代码以对在网格 11 外部的目标 341 和 343 发起攻击 351A 和 351B。

拒绝服务攻击的通常形式是:

缓冲器溢出攻击

最常见的 DoS 攻击的种类是简单地向一个网络地址发送这样多的流量，该流量比计划该网络地址的数据缓冲器的程序员所预期的某人可能发

送的流量更多。攻击者可能知道目标系统有能够利用的弱点，或者攻击者可以简单地尝试该攻击，以便该攻击可能万一有用。几种基于程序或系统的缓冲器特征的较知名的攻击包括:

- 发送带有含 256 个字符的文件名的附件的电子邮件消息到 Netscape 和 Microsoft 邮件程序
- 发送超尺寸的网际控制报文协议（ICMP）包（这也被称为死亡之包因特网或网际探测器（ping））
- 向 Pine 电子邮件程序的用户发送一个带有大于 256 个字符的“发件人”地址的消息

SYN 攻击

当启动一个在网络中的传输控制程序（TCP）客户端和服务器之间的会话时，存在一个很小的缓冲器空间以处理设定该会话的通常快速的“握手”消息交换。该些建立会话的包包括了一个识别该消息交换中的顺序的 SYN 字段。攻击者能够非常快速地发送若干连接请求，并接着对回复不作响应。这会使第一个包遗留在缓冲器中，以致无法接纳其他合法的连接请求。尽管在未收到回复的一个确定时间段后，缓冲器中的包会被丢弃，但是许多这样的伪造连接请求的影响使建立会话的合法请求变得困难。一般而言，此问题取决于操作系统提供正确设置，或者允许网络管理员调整缓冲器和超时时间段的大小。

泪珠攻击

此类拒绝服务攻击利用这样的方式: 网际协议（IP）要求一个对于下一个路由器太大而无法处理的包被分成片段。片段包识别相对于第一个包开始处的偏移量，该偏移量使整个包能够被接收系统重新组装。在泪珠攻击中，攻击者的 IP 在第二个或之后的片段中放置一个混淆的偏移量值。如果接收的操作系统没有对这种情况的计划，则该攻击能够导致系统崩溃。

Smurf 攻击

在 Smurf 攻击中，作恶者向接收站点发送一个 IP ping（或“将我的消息回送给我”）的请求。该 ping 包指定将它自己广播给在接收站点的本地网络内的若干主机。该包还指出该请求来自另一个站点，即将接收到拒绝服务的目标站点。（发送其中带有其他人的返回地址的包被称为哄骗返回地址。）结果将是大量的 ping 回复涌回无辜的、被哄骗的主机。如果该洪流足够强大，被哄骗的主机将不再能够接收或者区别真实的流量。

病毒

以各种方式遍布网络复制的计算机病毒可被看成拒绝服务攻击，在该攻击中，通常受害者不是特别作为目标的，而是简单地是一个不幸获得病毒的主机。取决于特定的病毒，拒绝服务可以是从几乎察觉不到一直到灾难性的。

僵尸攻击

在至少一种形式的拒绝服务攻击中，一个或多个不安全资产，如 PC、工作站或 Web 服务器，会被在每个中间目标中安置代码的恶意攻击者危害，当该中间目标被触发时会向被攻击的最终目标，典型地为一个目标网站，发起极大数量的攻击，例如服务请求。该最终目标很快将无法服务于来自它的用户的合法请求。一个被用于对最终目标发起 DDoS 攻击的攻击发起点的被危害的中间目标被称为僵尸。

通常的僵尸攻击包括试图淹没一个或多个目标计算机的一个稳定的（并因此更容易被跟踪的）攻击流量流，而一个脉冲式的僵尸攻击包括试图阻碍服务的不规则的流量猝发。定位来自脉冲式僵尸的攻击源或甚至知道该攻击已经发生是更加困难的。已知有脉冲式僵尸攻击在被检测到之前持续了数月之久；在一个情况下，受害者在几个月里接收了六倍于正常的流量。

d. 网格计算环境中的拒绝服务攻击

在 DDoS 攻击中网格和网格元件对成为可识别元件即中间目标或潜在僵尸的抵抗力是限制网格安装的商业部署的首要问题。至今为止，对于小的目标子集，DDoS 是代价非常大的。然而，迄今已认为僵尸的传播是在 IP 地址空间的多个和没有联系的部分中。出于此原因，应对僵尸负责的子网络管理员的任何有害的实践，例如没有表现出应有的留心，是无法被迅速识别的。

如上所述，有很多种 DDoS 攻击。一个简单的 DDoS 攻击可能是发往著名端口如端口 53（DNS）或端口 161（SNMP）的 TCP SYN 包的洪流、UDP 包的洪流、或者 ICMP PING 包的洪流。特别地，TCP SYN 的洪流已经是因特网商务风险中令人遗憾的部分。这就导致了诸如 TCP 粘合（TCP splicing）和防火墙加速器中巨大的连接表的对策。

与靠蛮力的洪流相对比，一种更复杂的 DDoS 可能与受害者建立一个 TCP 会话，接着通过从不完成的或者是有目的地残缺的端口 443（SSL HTTPS）安全会话初启程序淹没受害者。SSL 洪流攻击对于攻击者或者作恶者的重要优势是会需要少得多的资源。甚至一个大的 SSL 服务器每秒钟仅可以处理几千个 SSL 启动。这与在一个连接表中保持一百万个会话的防火墙加速器形成对比。

在所有 DDoS 攻击中的共同主题是征募僵尸，僵尸遵照一个信号（包括由操作系统生成的每日时间信号）向最终受害者发送如此大量特定类型的流量，以致淹没最终受害者的计算资源。

出于此原因，武器装备，即在分布式拒绝服务（DDoS）攻击中网格防止被用作可识别的实体（也就是中间目标或僵尸）的抵抗力，成为了一个设计、实现和部署的问题。

攻击者可能远程发现网格或它的元件的脆弱性，例如，通过发现许多具有相似的 IP 地址（或者在 NAP 存在时相同的 IP 地址）及许多开放的端口（可用并可响应）的机器。一般而言，这些不会是著名的端口号。例如，大多数 9000 至 32000 之间的端口号都不会是著名的端口号。

对于攻击者来说，也许显而易见的是，地址类似的机器也会有类似的操作系统、应用、服务包级别和补丁级别，并且因此具有相同的脆弱性。也就是说，一个许多节点的大型网格可能与 Windows 2000 机器的一整个网络在相同的意义上是脆弱的。对于一个攻击者，能够很快控制具有未修补的相同脆弱性的许多机器。这可以使用例如蠕虫感染或自动挖掘者（auto rooter）来完成。结果是很容易危害一个网格中的几台机器。在 DDoS 攻击的情况下，该攻击可以使被攻击的机器成为僵尸。

一旦网格中的元件被 DDoS 攻击接管，即可相对容易地证明许多或大多数的随后的传出攻击来自一个特定的网格。

于是，存在一种需求，来检测来自一个被感染的网格的传出的攻击流量，以便于识别、反应和补救，并限制此网格在随后的 DDoS 攻击中的参与。

此外，存在一种需求，来包括通过可表明 DDoS 攻击的统计方法识别在 DDoS 攻击中网格的参与，以便能够有效地和自动地响应 DDoS 攻击。

发明内容

本发明的目标是需要提供一种方法、系统和设备，来检测来自一个被感染的网格中的传出的攻击流量，以便于识别、反应和补救，并限制此网格在随后的 DDoS 攻击中的参与。

本发明进一步的目标是通过可表明 DDoS 攻击的统计手段识别在 DDoS 攻击中的网格参与，并因此使得能够有效地和自动地响应 DDoS 攻击。

本发明提供用于管理在多处理器环境中例如网格计算环境中由恶意代码发起的拒绝服务攻击的方法、系统和产品。这是通过对来自该多处理器环境中的传出的包的统计分析来实现的。第一步是建立多处理器环境中的正常流量使用的基线。一旦建立了该基线，下一步是监控传出的流量以检测被发送至特定目的地址的大比例的包，以及与基线相比的大量的传出包。下一步是监控端口和协议，以检测被发送至特定目标端口的大比例的包，

以及大多数或所有的发送至该最终目标端口的包对一个或少数几个协议的一致使用。如果存在这样的所有发送至该端口的包对一个协议的一致使用以至于证明了一个拒绝服务攻击，则启动阻止措施以减轻明显的拒绝服务攻击。

如这里所使用的，一个网格包括了任何被组织成为或能够被组织成为地址空间片（例如通过逻辑连接、部门、建筑物、业务单元、场所等等）的子网络，并且该子网络不一定为网格。可以监控子网络以发现 DDoS 攻击的指示。例如，通过流量特征能够将一个特定片与其他片区分开，并且在该片中，许多、大多数或甚至所有活动的机器具有近似相同的行为。以这种方式能够保护松散相关的一组资产（如处理器、节点、集线器和存储设备）。

附图说明

通过详细描述优选的实施例以及参考附图，本发明的以上目标和优势得以说明。

图 1 说明了一个网格 11。网格 11 包括一般地显示为工作站的五个元件：111、113、115、117 和 119。单个元件本身可以是网格、LAN、WAN、处理器。

图 2 说明了一个网格 11 及其元件 111、113、115、117 和 119，以及通过互联网 223 访问网格 11 的客户端工作站 221。

图 3 说明了一个网格 11 及其元件 111、113、115、117 和 119，以及通过因互联网 223 访问网格 11 以启动一个 DDoS 攻击 341 的客户端工作站 221，该 DDoS 攻击 341 通过在网格元件 115 和 117 中植入有害代码对最终目标即受害者 341 和 343 发起攻击 351A 和 351B。

图 4 是一个执行本发明的方法的示例流程图。

具体实施方式

本发明的目标是提供一种方法、系统和设备，以检测来自一个被感染

的网格的传出的攻击流量，以便于识别、反应和补救，并限制此网格在随后的 DDoS 攻击中的参与。DDoS 检测是通过对传入和传出数据流的统计分析完成的。

本发明提供了用于管理在多处理器环境中即网格环境中的拒绝服务攻击的方法、系统和产品。这是由通过对传入和传出流的统计分析来检测统计特征和统计异常完成的。第一步是建立在多处理器环境中的正常流量使用的基线。一旦建立了该基线，下一步是监控传出流量以检测被发送至特定目标地址（潜在的最终目标或受害者）的大比例的包，以及与所述基线相比的大量的传出包。下一步是监控端口和协议，以检测被发送至特定目标端口的大比例的包，以及大多数或所有的发送至该端口的包对一个协议的一致使用。如果存在这样的所有发送至该端口的包对一个协议的一致使用以至于证明了一个拒绝服务攻击，则启动阻止措施以减轻明显的拒绝服务攻击。

从一网格即从网格的一个或者多个元件例如一个或者几个子网络内的发起的拒绝服务攻击会显示某些流量特征。这些流量特征（这里“TC”指“流量特征”）包括:

TC1. 在攻击流量中见到的 IP 头部中的目的地址字段全部或几乎全部具有一个值或者少数几个值。

TC2. 在攻击流量中见到的 UDP 或 TCP 头部中的目的端口会具有一个值或者几个值。该端口可以是正确可用的服务的端口，如端口 80（WWW）或者端口 443（SSL）。在一些情况下，包长度可以是恒定的。

TC3. DDoS 流量会在恒定流或猝发流中具有很高的带宽。注意猝发流会更难被高度确定地检测到。注意，对于以恒定或者几乎恒定的流量为特征的 DDoS 攻击，DDoS 攻击的目的是通过使网络资源的处理能力或带宽过载以停止对网络资源的合法使用，并因此一定存在通向该目标的相对恒定的流量流。

TC4. 有些情况下，可存在高比率的 TCP 或 SSL 超时，导致了高比率的传入的 TCP RST 或 FIN 流量。一般而言，在海量的正常流量中，TCP

超时和 SSL 超时都不应出现。因而当大量看到这种超时时，证明了一个 DDoS。

TC5. 流量也可以是其他 254 种协议中的任何一种。带有 Protocol（IP 头部的 TYPE 字段）= 0 的洪流是常见的，ICMP 洪流也是正常的（Protocol = 1）。

能够认出两种统计异常。第一，很可能在子网络地址空间中有一个相邻的或者几乎相邻的发送这样的流量的地址片，该流量由 TC1...TC5 从来自该子网的所有其他流量中区别出来。第二，在存在 DDoS 攻击时，在该地址片中，不同机器的流量特征会非常类似。

一个典型的网格 11 显示于图 1 中。网格 11 包括一般地显示为工作站的五个元件：111、113、115、117 和 119。不过，单个元件本身可以是网格、LAN、WAN、处理器。图 2 说明了一个网格 11 及其元件 111、113、115、117 和 119，以及通过互联网 223 访问网格 11 的客户端工作站 221。

图 3 说明了网格 11（及一般地显示为工作站的元件 111、113、115、117 和 119），以及通过互联网 223 访问网格 11 以启动一个 DDoS 攻击 341 的客户端工作站 221，该 DDoS 攻击 341 通过在网格元件 115 和 117 中植入有害代码对目标 341 和 343 发起攻击 351A 和 351B。如图 3 所示，网格 11 正在受到 DDoS 攻击，以便由暗中植入处理器 115 和 117 的僵尸代码在处理器 341 和 343 上发动 DDoS 攻击。DDoS 可以是恐怖袭击、或勒索或敲诈阴谋、或仅仅是简单的恶意黑客行为。

本发明的实践开始于识别出在一个支持网格的子网络的传入和传出流量的正常流的中不寻常和异常地存在带有上述一种或多种异常流量特征的包的占优势的子集。异常流量的源地址可在一片完整地址空间之内，并且该片流量的统计值会非常不同于正常流量。此外，一片内的异常流量的统计值和流量特征可以在机器之间非常相似。

如上所述，有许多种 DDoS 攻击。一个简单的 DDoS 攻击可能是发往一个著名端口如端口 53（DNS）或 161（SNMP）的 TCP SYN 包的洪流、UDP 包的洪流、或者 ICMP PING 包的洪流。特别地，TCP SYN 洪流已

经是因特网商务风险中令人遗憾的一部分。这导致了诸如 TCP 接合和防火墙加速器中的巨大连接表的对策。

与靠蛮力的洪流相对比，一种更加复杂的 DDoS 可能与目标或最终受害者建立一个 TCP 会话，接着通过从不完成的或者是有目的地残缺的端口 443（SSL HTTPS）安全会话初启程序淹没该目标或最终受害者。SSL 洪流的重要优势是会需要少得多的资源（即中间目标或者僵尸）。甚至一个大的 SSL 服务器每秒钟仅仅能够处理几千个 SSL 启动。这与在一个连接表中拥有一百万个会话的防火墙加速器形成对比。

所有 DDoS 攻击中的一个共同主题是征募僵尸，僵尸遵照信号向受害者发送如此大量的特定类型的流量，以至于受害者的计算资源被淹没。

DDoS 攻击的检测和识别

将通过四类传出的 DDoS 攻击说明本发明。

TCP DDoS 攻击。对 TCP 攻击的检测会包括指向一个目的地或者少数几个目的地的异常数量的 SYN 流量。在 SYN、ACK、FIN 和 RST 这四种 TCP 标志中，必须有至少一种标志被设置（=1），并且在 SYN、FIN 和 RST 中，必须有至少一种标志被设置（=1）。在一个传出的 DDoS 中，可能有异常高水平的除 SYN 之外的 TCP 标志组合，包括非法的标志组合。TCP DDoS 攻击的另一个指示会是四种 TCP 标志的相互之间的典型比率的根本偏离。也就是说，应该有数量大致相等的 SYN 和 SYN/ACK。在一段长时期内，会有数量大致相等的 SYN 和 FIN。不应该存在相对于所有非 RST 的类型的过多数量的 RST。

ICMP 攻击。对 ICMP 攻击的检测会包括 Ping 包（其目的地端口（DP）=8）的过高水平。在一次成功的攻击中，传出的 Ping 包与传入的 Ping 回送包（其 DP=11）的比率会高于通常期望的 1 比 2 的比率。

UDP 攻击。对 UDP 攻击的检测会包括包的过高水平，这些包很可能具有一个 DP 或几个 DP 值。可能考虑 UDP 与 TCP 的比率，因为通常两者皆循环七天、每天二十四小时。

SSL（HTTPS）攻击。一个 SSL 攻击会包括正确启动一个 TCP 会话，但接着仅仅部分的 SSL 安全会话。某些 SSL 字段会故意成为不正确的或非法的。阻塞服务器所需的截短的 SSL 会话的数量可能大大低于造成同样效果所需的 TCP SYN 的数量。因此，对于 SSL DDoS 攻击，带宽会很高，例如相对于正常 SSL，每分钟超过 100 个启动的会话。如果 SSL 攻击嵌入所有其他流量中，特别是所有其他 TCP 流量中，这可能不会引人注意。因此，一个 SSL DDoS 可能包括 SSL 相对于其他 TCP 的过高的比率，或者 SSL 超时相对于所有 SSL 流量的过高的比率。

检测方法

有几个可用于以信号通知来自被监控的网格的中间目标或僵尸的传出网格攻击正在进行的主要的方法。这些检测方法基于确定流量类型、整个网格中的流量、以及一个或一小子集的子网络地址空间与其余子网络地址空间非常不同，例如在流量、流量类型或协议方面，但对于该小子集的子网络地址空间，不同机器之间的流量非常类似。

一个方法将是建立正常的流量并建立和定义基线。这些基线可包括协议使用（TCP、UDP 和 ICMP）和共同使用的服务（HTTP、HTTPS、MS-SQL-M、DNS 等等）的比例。与已建立的基线的比较会启动阻止措施以减缓可能的攻击。

具有图 4 所示的流程图的一种算法方法开始于监控关于目的地址的传出流量，方框 41。如果对某个目的地址的包的数量与全部传出包的数量的比率超过某个数字（如 0.5），并且全部传出包的数量超过一个预置值，方框 43，则监控选定的端口和协议，方框 45。例如，如果对一个端口的包的数量与对所有端口的全部包的数量的比率超过某个值（如 0.5），并且所使用的协议在所有或大部分的端口之间是一致的，方框 47，则开始阻止措施以阻止可能的攻击，方框 49。

应该注意到，过度依赖于对特定目的地址的包的数量与全部传出包的数量的比率超过某个数字（如 0.5）以及全部传出包的数量超过一个预置值，

能够导致错误的断言，并且管理员应该禁止持续的IP地址监控。这种情况是因为拒绝服务攻击常常持续很长的一段时间。因此，几个小时后达到的痛阈与比如96小时后的痛阈相比可能不显著，因而延迟动作以允许管理员交互是可行的。

另一个的检测工具是检测来自一片子网络地址空间的非正常比例的超时，检测来自该片子网络空间的流量与正常流量及该子网络中的其他元件的流量不同，或者检测在该片中的流量在该子网络内的不同机器之间具有不正常的高度一致性。

最普通的DDoS的情况将典型地包括在攻击流量中见到的IP头部中的目的地址字段均具有一个值或少数几个值，以及UDP或TCP头部中的目的端口具有一小组的值，如一个或几个值。另一方面，在ICMP攻击的情况中，ICMP 包的比例会异常之高。这意味着检测是通过认识到网格内的多台机器（转变为僵尸的中间目标）在同一端口攻击同一地址运行的。在这一点上，使用的端口也会意味着某个协议（如用于UDP的端口1434和用于TCP的端口80），这转而导致了完全不同的网格动作之间的较容易的提取和相关联。

阻止措施

所有现代的路由器和防火墙都能够在（在OSI协议栈中的）第4层过滤。这意味着能够指定过滤器规则以阻止（丢弃并报告）一个或几个IP源地址和一个或几个IP源端口的任何组合。在某些情况下，能够在申请服务、回复、口令请求、口令提交、识别、认证、授权的某种组合的一个握手系统的特定阶段，或任何密码过程中的任何部分（如公钥交换过程中的任何部分），对包应用更精密复杂的阻止。本发明使用了这样的阻止能力，但该阻止能力不包括在本发明中。

在一个实施例中，自动施加阻止措施会是施加行为的一个动态时期。

程序产品

本发明可以例如通过将用于管理拒绝服务攻击的系统作为一种软件应用（作为一个操作系统元件）、一种专用处理器、或一种带有专用代码的专用处理器来实现。该代码执行机器可读的一个指令序列，该指令序列也可称为代码。这些指令可驻留在各种类型的信号承载的媒介中。在这方面，本发明的一个方面涉及了一种程序产品，此程序产品包含一种或多种信号承载媒介，该媒介有形地体现了由一个数字处理设备执行以实现在多处理器环境中管理拒绝服务攻击的方法的机器可读指令的程序。

此信号传播媒介可包含例如服务器中的存储器。服务器中的该存储器可以是非易失性存储器、数据盘、或甚至是用于为了安装而下载到处理器的、厂商服务器上的存储器。除此之外，该些指令可体现在信号承载媒介例如数据存储光盘中。除此之外，该些指令可存储在多种机器可读数据存储媒介（mediums 或 media）中的任何一种上，该多种媒介包括，例如，“硬盘驱动器”、RAID 阵列、RAMAC、数据存储磁盘（如软盘）、磁带、数字光带、RAM、ROM、EPROM、EEPROM、闪速存储器、磁光存储器、穿孔纸卡片、或任何其他适合的信号承载媒介，包括传输媒介，例如可以是电的、光的和/或无线的数字和/或模拟通信链路。举例来说，机器可读指令可包含软件对象代码，该代码从一种语言例如“C++”、Java、Pascal、ADA、汇编程序等等编译。

此外，该程序代码可以例如被压缩、加密、或二者兼备，并可包括可执行文件、脚本文件和安装向导，如在 Zip 文件和 cab 文件中。如这里所使用的，术语“驻留在信号传播媒介其中或其上的机器可读指令或代码”包括了上面所有的交付方法。

其他实施例

虽然前述的公开内容显示了本发明的若干说明性的实施例，不过很显然，对于本领域的技术人员，无需背离由所附权利要求定义的本发明的范围即能够在这里实现各种变化和修改。此外，尽管本发明的元件可以作为单数描述和要求保护，不过除非清楚声明了单数的限制，复数也是可能的。

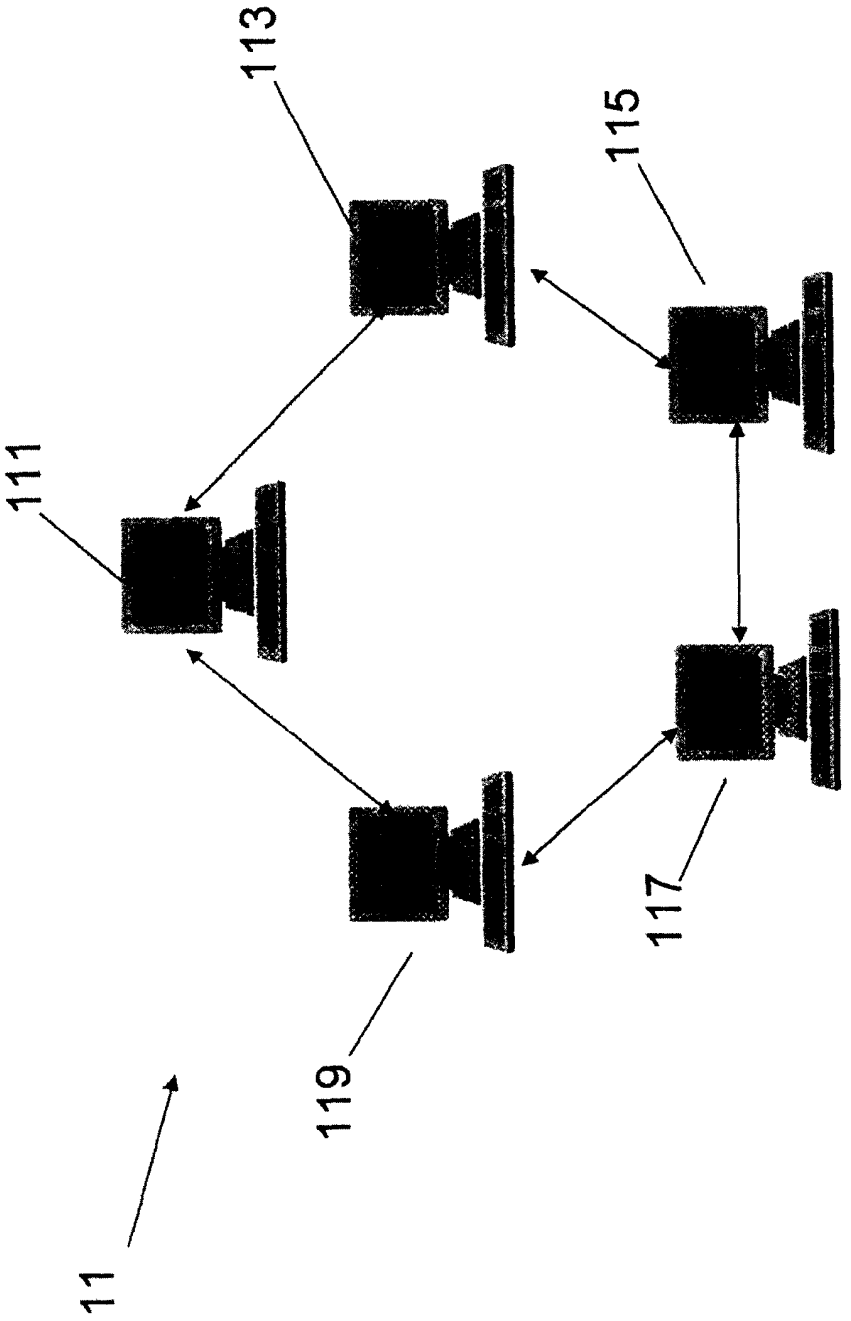


图 1

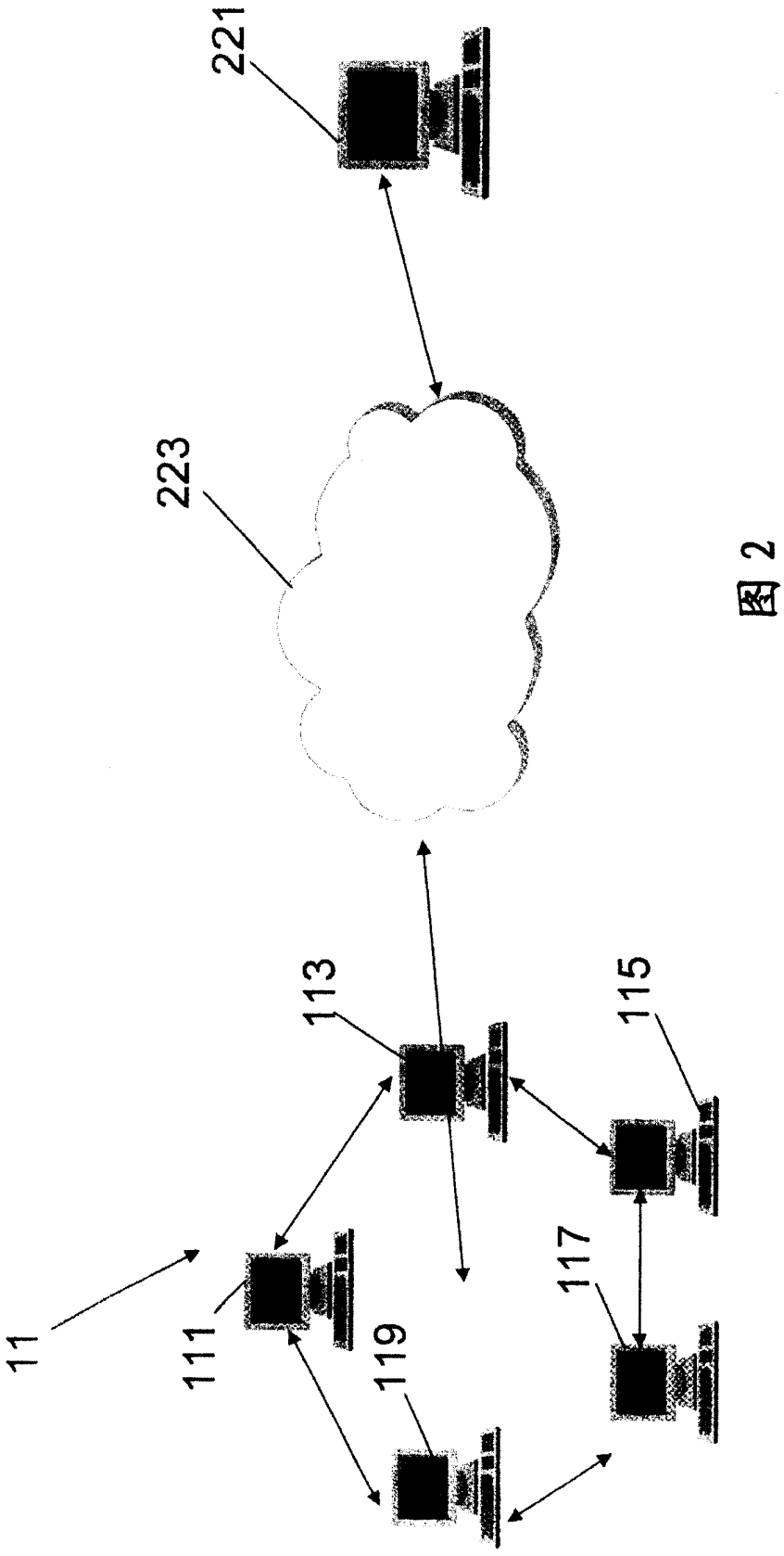


图 2

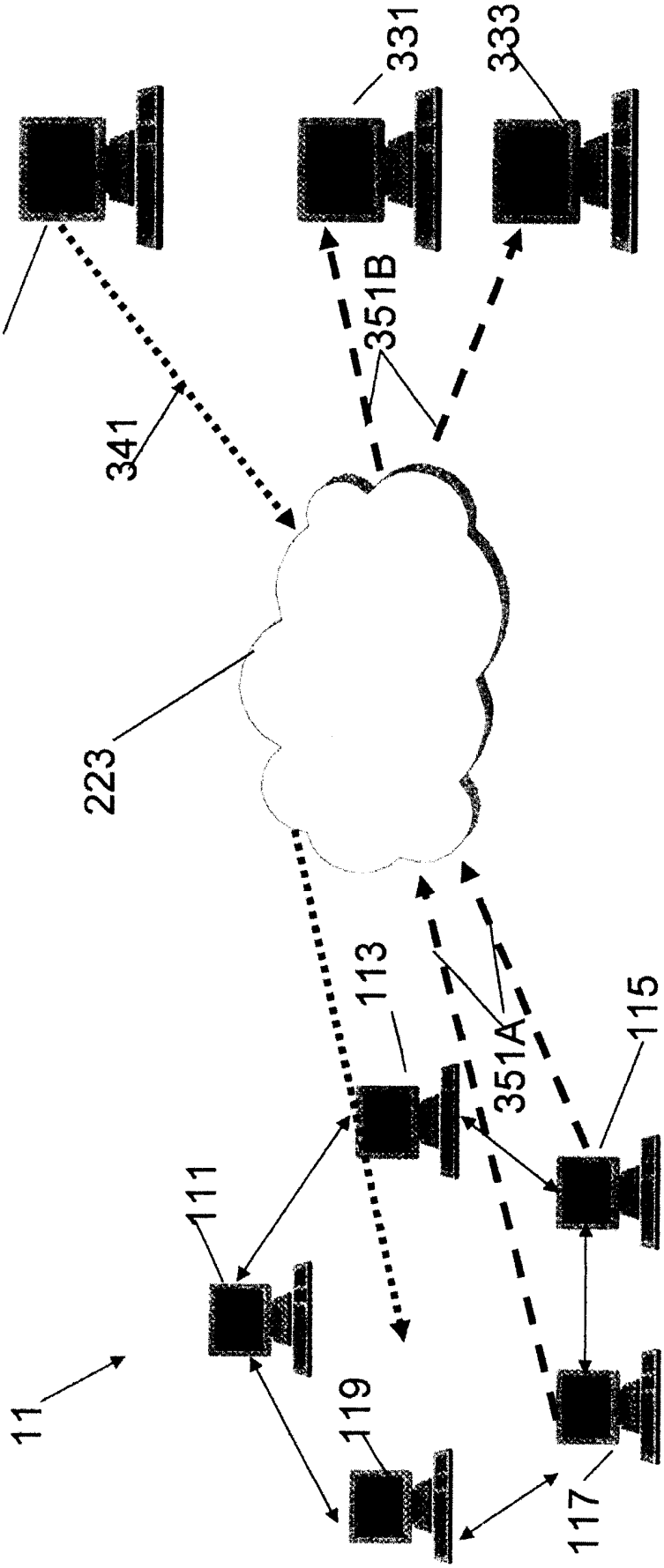


图 3

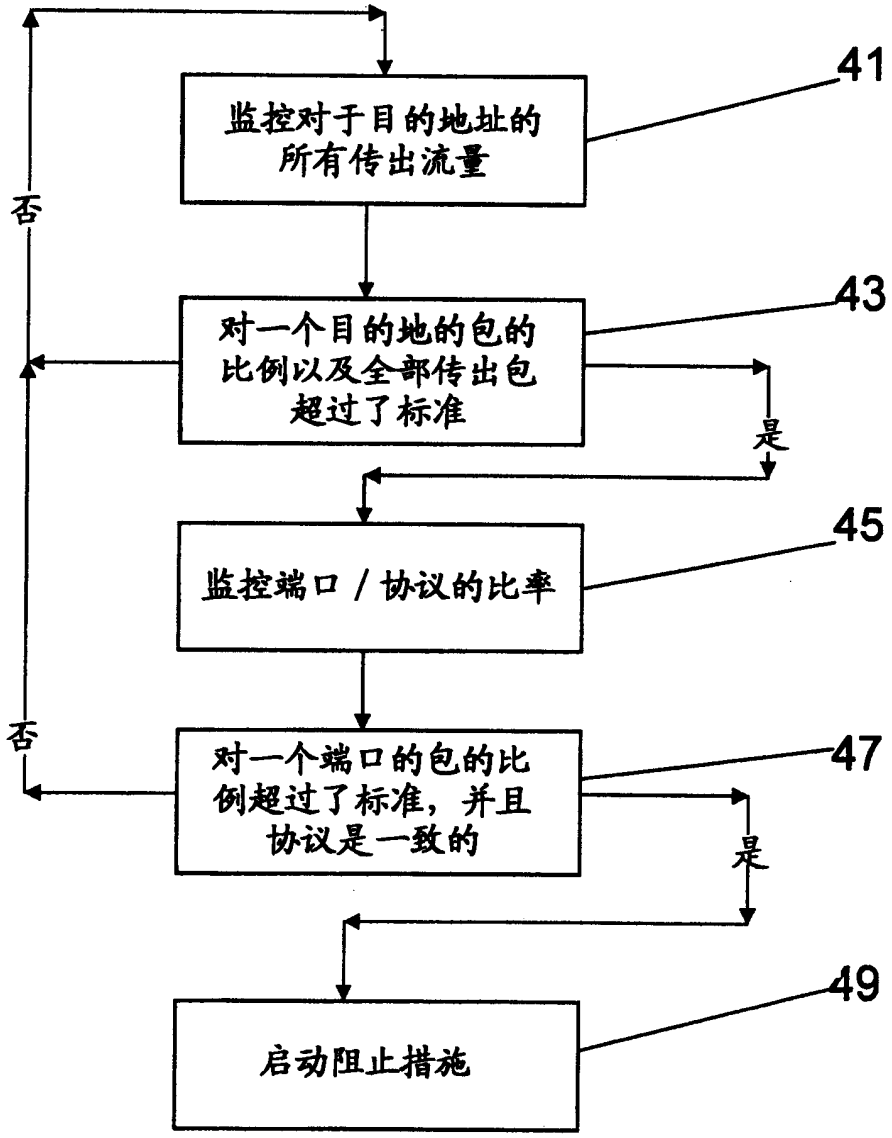

41
监控对于目的地址的所有传出流量
否
43
对一个目的地的包的比例以及全部传出包超过了标准
是
45
监控端口／协议的比率
否
47
对一个端口的包的比例超过了标准，并且协议是一致的
是
49
启动阻止措施

图 4